

GRID SECURITY RESEARCH AND DEVELOPMENT ACT

SEPTEMBER 4, 2020.—Ordered to be printed

Ms. JOHNSON of Texas, from the Committee on Science, Space, and
Technology, submitted the following

R E P O R T

[To accompany H.R. 5760]

[Including cost estimate of the Congressional Budget Office]

The Committee on Committee on Science, Space, and Technology, to whom was referred the bill (H.R. 5760) to provide for a comprehensive interdisciplinary research, development, and demonstration initiative to strengthen the capacity of the energy sector to prepare for and withstand cyber and physical attacks, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

	Page
I. Amendment	2
II. Purpose of the Bill	10
III. Background and Need for the Legislation	10
IV. Committee Hearings	10
V. Committee Consideration and Votes	11
VI. Summary of Major Provisions of the Bill	11
VII. Section-By-Section Analysis (By Title and Section)	11
VIII. Committee Views	13
IX. Cost Estimate	13
X. Congressional Budget Office Cost Estimate	13
XI. Compliance with Public Law 104-4 (Unfunded Mandates)	14
XII. Committee Oversight Findings and Recommendations	14
XIII. Statement on General Performance Goals and Objectives	15
XIV. Federal Advisory Committee Statement	15
XV. Duplication of Federal Programs	15
XVI. Earmark Identification	15
XVII. Applicability to the Legislative Branch	15
XVIII. Statement on Preemption of State, Local, or Tribal Law	15
XIX. Changes in Existing Law Made by the Bill, As Reported	15
XX. Exchange of Committee Correspondence	27
XXI. Proceedings of Full Committee Markup	29

I. AMENDMENT

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the “Grid Security Research and Development Act”.

SEC. 2. FINDINGS.

Congress finds the following:

- (1) The Nation, and every critical infrastructure sector, depends on reliable electricity.
- (2) Intelligent electronic devices, advanced analytics, and information systems used across the energy sector are essential to maintaining reliable operation of the electric grid.
- (3) The cybersecurity threat landscape is constantly changing and attacker capabilities are advancing rapidly, requiring ongoing modifications, advancements, and investments in technologies and procedures to maintain security.
- (4) It is in the national interest for Federal agencies to invest in cybersecurity research that informs and facilitates private sector investment and use of advanced cybersecurity tools and procedures to protect information systems.
- (5) The number of devices and systems connecting to the electric grid is increasing, and integrating cybersecurity protections into information systems when they are built is more effective than modifying products after installation to meet cybersecurity goals.
- (6) An understanding of human factors can be leveraged to understand the behavior of cyber threat actors, develop strategies to counter threat actors, improve cybersecurity training programs, optimize the design of human-machine interfaces and cybersecurity tools, and increase the capacity of the energy sector workforce to prevent unauthorized access to critical systems.

SEC. 3. AMENDMENT TO ENERGY INDEPENDENCE AND SECURITY ACT OF 2007.

Title XIII of the Energy Independence and Security Act of 2007 (42 U.S.C. 17381 et seq.) is amended by adding at the end the following:

“SEC. 1310. ENERGY SECTOR SECURITY RESEARCH, DEVELOPMENT, AND DEMONSTRATION PROGRAM.

“(a) IN GENERAL.—The Secretary, in coordination with appropriate Federal agencies, the Electricity Subsector Coordinating Council, the Electric Reliability Organization, State, tribal, local, and territorial governments, the private sector, and other relevant stakeholders, shall carry out a research, development, and demonstration program to protect the electric grid and energy systems, including assets connected to the distribution grid, from cyber and physical attacks by increasing the cyber and physical security capabilities of the energy sector and accelerating the development of relevant technologies and tools.

“(b) DEPARTMENT OF ENERGY.—As part of the initiative described in subsection (a), the Secretary shall award research, development, and demonstration grants to—

- “(1) identify cybersecurity risks to information systems within, and impacting, the electricity sector, energy systems, and energy infrastructure;
- “(2) develop methods and tools to rapidly detect cyber intrusions and cyber incidents, including through the use of data and big data analytics techniques, such as intrusion detection, and security information and event management systems, to validate and verify system behavior;
- “(3) assess emerging cybersecurity capabilities that could be applied to energy systems and develop technologies that integrate cybersecurity features and procedures into the design and development of existing and emerging grid technologies, including renewable energy, storage, and demand-side management technologies;
- “(4) identify existing vulnerabilities in intelligent electronic devices, advanced analytics systems, and information systems;
- “(5) work with relevant entities to develop technologies or concepts that build or retrofit cybersecurity features and procedures into—
 - “(A) information and energy management system devices, components, software, firmware, and hardware, including distributed control and management systems, and building management systems;
 - “(B) data storage systems, data management systems, and data analysis processes;
 - “(C) automated- and manually-controlled devices and equipment for monitoring and stabilizing the electric grid;

“(D) technologies used to synchronize time and develop guidance for operational contingency plans when time synchronization technologies, are compromised;

“(E) power system delivery and end user systems and devices that connect to the grid, including—

“(i) meters, phasor measurement units, and other sensors;

“(ii) distribution automation technologies, smart inverters, and other grid control technologies;

“(iii) distributed generation, energy storage, and other distributed energy technologies;

“(iv) demand response technologies;

“(v) home and building energy management and control systems;

“(vi) electric and plug-in hybrid vehicles and electric vehicle charging systems; and

“(vii) other relevant devices, software, firmware, and hardware; and

“(F) the supply chain of electric grid management system components;

“(6) develop technologies that improve the physical security of information systems, including remote assets;

“(7) integrate human factors research into the design and development of advanced tools and processes for dynamic monitoring, detection, protection, mitigation, response, and cyber situational awareness;

“(8) evaluate and understand the potential consequences of practices used to maintain the cybersecurity of information systems and intelligent electronic devices;

“(9) develop or expand the capabilities of existing cybersecurity test beds to simulate impacts of cyber attacks and combined cyber-physical attacks on information systems and electronic devices, including by increasing access to existing and emerging test beds for cooperative utilities, utilities owned by a political subdivision of a State, such as municipally-owned electric utilities, and other relevant stakeholders; and

“(10) develop technologies that reduce the cost of implementing effective cybersecurity technologies and tools, including updates to these technologies and tools, in the energy sector.

“(c) NATIONAL SCIENCE FOUNDATION.—The National Science Foundation, in coordination with other Federal agencies as appropriate, shall through its cybersecurity research and development programs—

“(1) support basic research to advance knowledge, applications, technologies, and tools to strengthen the cybersecurity of information systems, including electric grid and energy systems, including interdisciplinary research in—

“(A) evolutionary systems, theories, mathematics, and models;

“(B) economic and financial theories, mathematics, and models; and

“(C) big data analytical methods, mathematics, computer coding, and algorithms; and

“(2) support cybersecurity education and training focused on information systems for the electric grid and energy workforce, including through the Advanced Technological Education program, the Cybercorps program, graduate research fellowships, and other appropriate programs.

“(d) DEPARTMENT OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY DIRECTORATE.—The Science and Technology Directorate of the Department of Homeland Security shall coordinate with the Department of Energy, the private sector, and other relevant stakeholders, to research existing cybersecurity technologies and tools used in the defense industry in order to—

“(1) identify technologies and tools that may meet civilian energy sector cybersecurity needs;

“(2) develop a research strategy that incorporates human factors research findings to guide the modification of defense industry cybersecurity tools for use in the civilian sector;

“(3) develop a strategy to accelerate efforts to bring modified defense industry cybersecurity tools to the civilian market; and

“(4) carry out other activities the Secretary of Homeland Security considers appropriate to meet the goals of this subsection.

“SEC. 1311. GRID RESILIENCE AND EMERGENCY RESPONSE.

“(a) IN GENERAL.—Not later than 180 days after the enactment of the Grid Security Research and Development Act, the Secretary shall establish a research, development, and demonstration program to enhance resilience and strengthen emergency response and management pertaining to the energy sector.

“(b) GRANTS.—The Secretary shall award grants to eligible entities under subsection (c) on a competitive basis to conduct research and development with the purpose of improving the resilience and reliability of electric grid by—

“(1) developing methods to improve community and governmental preparation for and emergency response to large-area, long-duration electricity interruptions, including through the use of energy efficiency, storage, and distributed generation technologies;

“(2) developing tools to help utilities and communities ensure the continuous delivery of electricity to critical facilities;

“(3) developing tools to improve coordination between utilities and relevant Federal agencies to enable communication, information-sharing, and situational awareness in the event of a physical or cyber-attack on the electric grid;

“(4) developing technologies and capabilities to withstand and address the current and projected impact of the changing climate on energy sector infrastructure, including extreme weather events and other natural disasters;

“(5) developing technologies capable of early detection of malfunctioning electrical equipment on the transmission and distribution grid, including detection of spark ignition causing wildfires and risks of vegetation contact;

“(6) assessing upgrades and additions needed to energy sector infrastructure due to projected changes in the energy generation mix and energy demand; and

“(7) upgrading tools used to estimate the costs of outages longer than 24 hours.

“(8) developing tools and technologies to assist with the planning, safe execution of, and safe and timely restoration of power after emergency power shut offs, such as those conducted to reduce risks of wildfires started by grid infrastructure.

“(c) ELIGIBLE ENTITIES.—The entities eligible to receive grants under this section include—

“(1) an institution of higher education;

“(2) a nonprofit organization;

“(3) a National Laboratory;

“(4) a unit of State, local, or tribal government;

“(5) an electric utility or electric cooperative;

“(6) a retail service provider of electricity;

“(7) a private commercial entity;

“(8) a partnership or consortium of 2 or more entities described in subparagraphs (1) through (7); and

“(9) any other entities the Secretary deems appropriate.

“(d) RELEVANT ACTIVITIES.—Grants awarded under subsection (b) shall include funding for research and development activities related to the purpose described in subsection (b), such as—

“(1) development of technologies to use distributed energy resources, such as solar photovoltaics, energy storage systems, electric vehicles, and microgrids, to improve grid and critical end-user resilience;

“(2) analysis of non-technical barriers to greater integration and use of technologies on the distribution grid;

“(3) analysis of past large-area, long-duration electricity interruptions to identify common elements and best practices for electricity restoration, mitigation, and prevention of future disruptions;

“(4) development of advanced monitoring, analytics, operation, and controls of electric grid systems to improve electric grid resilience;

“(5) analysis of technologies, methods, and concepts that can improve community resilience and survivability of frequent or long-duration power outages;

“(6) development of methodologies to maintain cybersecurity during restoration of energy sector infrastructure and operation;

“(7) development of advanced power flow control systems and components to improve electric grid resilience; and

“(8) any other relevant activities determined by the Secretary.

“(e) TECHNICAL ASSISTANCE.—

“(1) IN GENERAL.—The Secretary shall provide technical assistance to eligible entities for the commercial application of technologies to improve the resilience of the electric grid and commercial application of technologies to help entities develop plans for preventing and recovering from various power outage scenarios at the local, regional, and State level.

“(2) TECHNICAL ASSISTANCE PROGRAM.—The commercial application technical assistance program established in paragraph (1) shall include assistance to eligible entities for—

“(A) the commercial application of technologies developed from the grant program established in subsection (b), including cooperative utilities and

utilities owned by a political subdivision of a State, such as municipally-owned electric utilities;

“(B) the development of methods to strengthen or otherwise mitigate adverse impacts on electric grid infrastructure against natural hazards;

“(C) the use of Department data and modeling tools for various purposes;

“(D) a resource assessment and analysis of future demand and distribution requirements, including development of advanced grid architectures and risk analysis; and

“(E) the development of tools and technologies to coordinate data across relevant entities to promote resilience and wildfire prevention in the planning, design, construction, operation, and maintenance of transmission infrastructure;

“(F) analysis to predict the likelihood of extreme weather events to inform the planning, design, construction, operation, and maintenance of transmission infrastructure in consultation with the National Oceanic and Atmospheric Administration; and

“(G) the commercial application of relevant technologies, such as distributed energy resources, microgrids, or other energy technologies, to establish backup power for users or facilities affected by emergency power shutoffs.

“(3) ELIGIBLE ENTITIES.—The entities eligible to receive technical assistance for commercial application of technologies under this section include—

“(A) representatives of all sectors of the electric power industry, including electric utilities, trade organizations, and transmission and distribution system organizations, owners, and operators;

“(B) State and local governments and regulatory authorities, including public utility commissions;

“(C) tribal and Alaska Native governmental entities;

“(D) partnerships among entities under subparagraphs (A) through (C);

“(E) regional partnerships; and

“(F) any other entities the Secretary deems appropriate.

“(4) AUTHORITY.—Nothing in this section shall authorize the Secretary to require any entity to adopt any model, tool, technology, plan, analysis, or assessment.

“SEC. 1312. BEST PRACTICES AND GUIDANCE DOCUMENTS FOR ENERGY SECTOR CYBERSECURITY RESEARCH.

“(a) IN GENERAL.—The Secretary, in coordination with appropriate Federal agencies, the Electricity Subsector Coordinating Council, standards development organizations, State, tribal, local, and territorial governments, the private sector, public utility commissions, and other relevant stakeholders, shall coordinate the development of guidance documents for research, development, and demonstration activities to improve the cybersecurity capabilities of the energy sector through participating agencies. As part of these activities, the Secretary shall—

“(1) facilitate stakeholder involvement to update—

“(A) the Roadmap to Achieve Energy Delivery Systems Cybersecurity;

“(B) the Cybersecurity Procurement Language for Energy Delivery Systems, including developing guidance for—

“(i) contracting with third parties to conduct vulnerability testing for information systems used across the energy production, delivery, storage, and end use systems;

“(ii) contracting with third parties that utilize transient devices to access information systems; and

“(iii) managing supply chain risks; and

“(C) the Electricity Subsector Cybersecurity Capability Maturity Model, including the development of metrics to measure changes in cybersecurity readiness; and

“(2) develop voluntary guidance to improve digital forensic analysis capabilities, including—

“(A) developing standardized terminology and monitoring processes; and

“(B) utilizing human factors research to develop more effective procedures for logging incident events; and

“(3) work with the National Science Foundation, Department of Homeland Security, and stakeholders to develop a mechanism to anonymize, aggregate, and share the testing results from cybersecurity test beds to facilitate technology improvements by public and private sector researchers.

“(b) BEST PRACTICES.—The Secretary, in collaboration with the Director of the National Institute of Standards and Technology and other appropriate Federal agencies, shall convene relevant stakeholders and facilitate the development of—

“(1) consensus-based best practices to improve cybersecurity for—

“(A) emerging energy technologies;

“(B) distributed generation and storage technologies, and other distributed energy resources;

“(C) electric vehicles and electric vehicle charging stations; and

“(D) other technologies and devices that connect to the electric grid;

“(2) recommended cybersecurity designs and technical requirements that can be used by the private sector to design and build interoperable cybersecurity features into technologies that connect to the electric grid, including networked devices and components on distribution systems; and

“(3) technical analysis that can be used by the private sector in developing best practices for test beds and test bed methodologies that will enable reproducible testing of cybersecurity protections for information systems, electronic devices, and other relevant components, software, and hardware across test beds.

“(c) REGULATORY AUTHORITY.—None of the activities authorized in this section shall be construed to authorize regulatory actions. Additionally, the voluntary standards developed under this section shall not duplicate or conflict with mandatory reliability standards.

“SEC. 1313. VULNERABILITY TESTING AND TECHNICAL ASSISTANCE TO IMPROVE CYBERSECURITY.

“(a) IN GENERAL.—The Secretary shall—

“(1) coordinate with energy sector asset owners and operators, leveraging the research facilities and expertise of the National Laboratories, to assist entities in developing testing capabilities by—

“(A) utilizing a range of methods to identify vulnerabilities in physical and cyber systems;

“(B) developing cybersecurity risk assessment tools and providing analyses and recommendations to participating stakeholders; and

“(C) working with stakeholders to develop methods to share anonymized and aggregated test results to assist relevant stakeholders in the energy sector, researchers, and the private sector to advance cybersecurity efforts, technologies, and tools;

“(2) collaborate with relevant stakeholders, including public utility commissions, to—

“(A) identify information, research, staff training, and analytical tools needed to evaluate cybersecurity issues and challenges in the energy sector; and

“(B) facilitate the sharing of information and the development of tools identified under subparagraph (A);

“(3) collaborate with tribal governments to identify information, research, and analysis tools needed by tribal governments to increase the cybersecurity of energy assets within their jurisdiction.

“SEC. 1314. EDUCATION AND WORKFORCE TRAINING RESEARCH AND STANDARDS.

“(a) IN GENERAL.—The Secretary shall support the development of a cybersecurity workforce through a program that—

“(1) facilitates collaboration between undergraduate and graduate students, researchers at the National Laboratories, and the private sector;

“(2) prioritizes science and technology in areas relevant to the mission of the Department of Energy through the design and application of cybersecurity technologies;

“(3) develops, or facilitates private sector development of, voluntary cybersecurity training and retraining standards, lessons, and recommendations for the energy sector that minimize duplication of cybersecurity compliance training programs; and

“(4) maintains a public database of cybersecurity education, training, and certification programs.

“(b) GRID RESILIENCE TECHNOLOGY TRAINING.—The Secretary shall support the development of the grid workforce through a training program that prioritizes activities that enhance the resilience of the electric grid and energy sector infrastructure, including training on the use of tools, technologies, and methods developed under the grant program established in section 1311(b).

“(c) COLLABORATION.—In carrying out the program authorized in subsection (a) and (b), the Secretary shall leverage programs and activities carried out across the Department of Energy, other relevant Federal agencies, institutions of higher education, and other appropriate entities best suited to provide national leadership on cybersecurity and grid resilience-related issues.

“SEC. 1315. INTERAGENCY COORDINATION AND STRATEGIC PLAN FOR ENERGY SECTOR CYBERSECURITY RESEARCH.

“(a) DUTIES.—The Secretary, in coordination with the Energy Sector Government Coordinating Council, shall—

“(1) review the most recent versions of the Roadmap to Achieve Energy Delivery Systems Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity to identify crosscutting energy sector cybersecurity research needs and opportunities for collaboration among Federal agencies and other relevant stakeholders;

“(2) identify interdisciplinary research, technology, and tools that can be applied to cybersecurity challenges in the energy sector;

“(3) identify technology transfer opportunities to accelerate the development and commercial application of novel cybersecurity technologies, systems, and processes in the energy sector; and

“(4) develop a coordinated Interagency Strategic Plan for research to advance cybersecurity capabilities used in the energy sector that builds on the Roadmap to Achieve Energy Delivery Systems in Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity.

“(b) INTERAGENCY STRATEGIC PLAN.—

“(1) SUBMITTAL.—The Interagency Strategic Plan developed under subsection (a)(4) shall be submitted to Congress and made public within 12 months after the date of enactment of the Grid Security Research and Development Act.

“(2) CONTENTS.—The Interagency Strategic Plan shall include—

“(A) an analysis of how existing cybersecurity research efforts across the Federal Government are advancing the goals of the Roadmap to Achieve Energy Delivery Systems Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity;

“(B) recommendations for research areas that may advance the cybersecurity of the energy sector;

“(C) an overview of existing and proposed public and private sector research efforts that address the topics outlined in paragraph (3); and

“(D) an overview of needed support for workforce training in cybersecurity for the energy sector.

“(3) CONSIDERATIONS.—In developing the Interagency Strategic Plan, the Secretary, in coordination with the Energy Sector Government Coordinating Council, shall consider—

“(A) opportunities for human factors research to improve the design and effectiveness of cybersecurity devices, technologies, tools, processes, and training programs;

“(B) contributions of other disciplines to the development of innovative cybersecurity procedures, devices, components, technologies, and tools;

“(C) opportunities for technology transfer programs to facilitate private sector development of cybersecurity procedures, devices, components, technologies, and tools for the energy sector;

“(D) broader applications of the work done by relevant Federal agencies to advance the cybersecurity of information systems and data analytics systems for the energy sector; and

“(E) activities called for in the Federal cybersecurity research and development strategic plan required by section 201(a)(1) of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7431(a)(1)).

“(c) PARTICIPATION.—For the purposes of carrying out this section, the Energy Sector Government Coordinating Council shall include representatives from Federal agencies with expertise in the energy sector, information systems, data analytics, cyber and physical systems, engineering, human factors research, human-machine interfaces, high performance computing, big data and data analytics, or other disciplines considered appropriate by the Council Chair.

“SEC. 1316. REPORT TO CONGRESS.

“(a) BALANCING RISKS, INCREASING SECURITY, AND IMPROVING MODERNIZATION.—

“(1) STUDY.—The Secretary, in collaboration with the National Institute of Standards and Technology, other Federal agencies, and energy sector stakeholders, in order to provide recommendations for additional research, development, demonstration, and commercial application activities, shall—

“(A) analyze physical and cyber attacks on energy sector infrastructure and information systems and identify cost-effective opportunities to improve physical and cyber security; and

“(B) examine the risks associated with increasing penetration of digital technologies in grid networks, particularly on the distribution grid.

“(2) CONTENT.—The study shall—

“(A) analyze processes, operational procedures, and other factors common among cyber attacks;

“(B) identify areas where human behavior plays a critical role in maintaining or compromising the security of a system;

“(C) recommend—

“(i) changes to the design of devices, human-machine interfaces, technologies, tools, processes, or procedures to optimize security that do not require a change in human behavior; and

“(ii) training techniques to increase the capacity of employees to actively identify, prevent, or neutralize the impact of cyber attacks;

“(D) evaluate existing engineering and technical design criteria and guidelines that incorporate human factors research findings, and recommend criteria and guidelines for cybersecurity tools that can be used to develop display systems for cybersecurity monitoring, such as alarms, user-friendly displays, and layouts;

“(E) evaluate the cybersecurity risks and benefits of various design and architecture options for energy sector systems, networked grid systems and components, and automation systems, including consideration of—

“(i) designs that include both digital and analog control devices and technologies;

“(ii) different communication technologies used to transfer information and data between control system devices, technologies, and system operators;

“(iii) automated and human-in-the-loop devices and technologies;

“(iv) programmable versus nonprogrammable devices and technologies;

“(v) increased redundancy using dissimilar cybersecurity technologies; and

“(vi) grid architectures that use autonomous functions to limit control vulnerabilities; and

“(F) recommend methods or metrics to document changes in risks associated with system designs and architectures.

“(3) CONSULTATION.—In conducting the study, the Secretary shall consult with energy sector stakeholders, academic researchers, the private sector, and other relevant stakeholders.

“(4) REPORT.—Not later than 24 months after the date of enactment of the Grid Security Research and Development Act, the Secretary shall submit the study to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Energy and Natural Resources of the Senate.

“SEC. 1317. DEFINITIONS.

“In this title:

“(1) BIG DATA.—The term ‘big data’ means datasets that require advanced analytical methods for their transformation into useful information.

“(2) CYBERSECURITY.—The term ‘cybersecurity’ means protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

“(3) CYBERSECURITY THREAT.—The term ‘cybersecurity threat’ has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

“(4) ELECTRICITY SUBSECTOR COORDINATING COUNCIL.—The term ‘Electricity Subsector Coordinating Council’ means the self-organized, self-governed council consisting of senior industry representatives to serve as the principal liaison between the Federal Government and the electric power sector and to carry out the role of the Sector Coordinating Council as established in the National Infrastructure Protection Plan for the electricity subsector.

“(5) ENERGY SECTOR GOVERNMENT COORDINATING COUNCIL.—The term ‘Energy Sector Government Coordinating Council’ means the council consisting of representatives from relevant Federal Government agencies to provide effective coordination of energy sector efforts to ensure a secure, reliable, and resilient energy infrastructure and to carry out the role of the Government Coordinating Council as established in the National Infrastructure Protection Plan for the energy sector.

“(6) HUMAN FACTORS RESEARCH.—The term ‘human factors research’ means research on human performance in social and physical environments, and on the integration and interaction of humans with physical systems and computer hardware and software.

“(7) HUMAN-MACHINE INTERFACES.—The term ‘human-machine interfaces’ means technologies that present information to an operator or user about the state of a process or system, or accept human instructions to implement an action, including visualization displays such as a graphical user interface.

“(8) INFORMATION SYSTEM.—The term ‘information system’—

“(A) has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and

“(B) includes operational technology, information technology, and communications.

“(9) NATIONAL LABORATORY.—The term ‘national laboratory’ has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

“(10) SECURITY VULNERABILITY.—The term ‘security vulnerability’ has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

“(11) TRANSIENT DEVICES.—The term ‘transient devices’ means removable media, including floppy disks, compact disks, USB flash drives, external hard drives, mobile devices, and other devices that utilize wireless connections.

“SEC. 1318. AUTHORIZATION OF APPROPRIATIONS.

“There are authorized to be appropriated to the Secretary to carry out this Act—

“(1) \$150,000,000 for fiscal year 2021;

“(2) \$157,500,000 for fiscal year 2022;

“(3) \$165,375,000 for fiscal year 2023;

“(4) \$173,645,000 for fiscal year 2024; and

“(5) \$182,325,000 for fiscal year 2025.”.

SEC. 4. CRITICAL INFRASTRUCTURE RESEARCH AND CONSTRUCTION.

(a) IN GENERAL.—The Secretary shall carry out a program of research, development, and demonstration of technologies and tools to help ensure the resilience and security of critical integrated grid infrastructures.

(b) CRITICAL INFRASTRUCTURE DEFINED.—The term “critical infrastructure” means infrastructure that the Secretary determines to be vital to socioeconomic activities such that, if destroyed or damaged, such destruction or damage could cause substantial disruption to such socioeconomic activities.

(c) COORDINATION.—In carrying out the program under subsection (a), the Secretary shall leverage expertise and resources of and facilitate collaboration and coordination between—

(1) relevant programs and activities across the Department;

(2) the Department of Defense; and

(3) the Department of Homeland Security.

(d) CRITICAL INFRASTRUCTURE TEST FACILITY.—In carrying out the program under subsection (a), the Secretary shall establish and operate a Critical Infrastructure Test Facility (referred to in this section as the “Test Facility”) that allows for scalable physical and cyber performance testing to be conducted on industry-scale critical infrastructure systems. This facility shall include a focus on—

(1) cybersecurity test beds; and

(2) electric grid test beds.

(e) SELECTION.—The Secretary shall select the Test Facility under this section on a competitive, merit-reviewed basis. The Secretary shall consider applications from National Laboratories, institutions of higher education, multi-institutional collaborations, and other appropriate entities.

(f) DURATION.—The Test Facility established under this section shall receive support for a period of not more than 5 years, subject to the availability of appropriations.

(g) RENEWAL.—Upon the expiration of any period of support of the Test Facility, the Secretary may renew support for the Test Facility, on a merit-reviewed basis, for a period of not more than 5 years.

(h) TERMINATION.—Consistent with the existing authorities of the Department, the Secretary may terminate the Test Facility for cause during the performance period.

SEC. 5. CONFORMING AMENDMENT.

Section 1(b) of the Energy Independence and Security Act of 2007 is amended in the table of contents by adding after the matter relating to section 1309 the following:

“Sec. 1310. Energy sector security research, development, and demonstration program.

“Sec. 1311. Grid resilience and emergency response.

“Sec. 1312. Best practices and guidance documents for energy sector cybersecurity research.

“Sec. 1313. Vulnerability testing and technical assistance to improve cybersecurity.

“Sec. 1314. Education and workforce training research and standards.

“Sec. 1315. Interagency coordination and strategic plan for energy sector cybersecurity research.

“Sec. 1316. Report to Congress.
 “Sec. 1317. Definitions.
 “Sec. 1318. Authorization of appropriations.”.

II. PURPOSE OF THE BILL

The purpose of the bill is to authorize a comprehensive interdisciplinary research, development, and demonstration initiative to strengthen the capacity of the energy sector to prepare for and withstand cyber and physical attacks and improve the security of the energy sector. H.R. 5760 is sponsored by Mr. Bera and co-sponsored by Mr. Weber.

III. BACKGROUND AND NEED FOR THE LEGISLATION

The electric grid is a central and pivotal part of our quality of life, economy, and national security. The nation, and every critical infrastructure sector, depends on reliable electricity. However, the cybersecurity threat landscape faced by the energy sector is constantly changing and attacker capabilities are advancing rapidly, requiring ongoing modifications, advancements, and investments in technologies and procedures to maintain the security of these systems. Cyber and physical attacks on the grid are serious and require a sustained investment in research to keep pace with constantly shifting threats. Additionally, robust cybersecurity requires a highly skilled workforce that can quickly adapt to this threat landscape. The Department of Energy (DOE) has an important role to play in developing relevant technologies and other supporting programs to achieve these goals.

DOE’s Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads the Department’s efforts on emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyber-attacks, natural disasters, and man-made events. CESER supports improving cybersecurity preparedness in the energy sector; coordinating responses and recovery from cyber incidents; detecting and mitigating cyber risks for energy sector owners and operators; and sharing threat information among energy sector partners, in addition to a variety of other activities. CESER partners with other federal agencies, including the Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), and National Science Foundation (NSF), and industry partners in carrying out its mission.

IV. COMMITTEE HEARINGS

Pursuant to Section 103(i) of H. Res. 6, the Committee designates the following hearings as having been used to develop or consider the legislation:

On July 17, 2019 the Honorable Conor Lamb presiding, the Subcommittee on Energy of the Committee on Science, Space, and Technology held a hearing to examine research needs to modernize and secure our nation’s electricity grid. Witnesses and Members discussed the extensive work done at DOE to develop technologies that improve the flexibility, resilience, and security of the electric grid and the need for continued and additional investments in our nation’s cybersecurity and emergency response workforce.

WITNESSES

The Honorable Karen Evans, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy

Mr. Juan J. Torres, Associate Laboratory Director, Energy Systems Integration, National Renewable Energy Laboratory and Co-Chair, Grid Modernization Lab Consortium

Ms. Kelly Speakes-Backman, CEO, Energy Storage Association

Ms. Katherine Hamilton, Chair, 38 North Solutions and Executive Director, Advanced Energy Management Alliance

V. COMMITTEE CONSIDERATION AND VOTES

The Committee on Science, Space, and Technology met to consider H.R. 5760 on February 12, 2020, and considered the following amendments to the bill:

Mr. Bera offered a Manager’s amendment that would make technical and conforming changes to the bill. *The amendment was agreed to by a voice vote.*

Mr. McNerney offered an amendment that would ensure the Secretary would support the research and development of tools and technologies to prevent wildfires caused by electric grid infrastructure and would also support the development of training programs for the grid infrastructure workforce. *The amendment was agreed to by a voice vote.*

Mr. Waltz offered an amendment that would add a research, development, and demonstration program to advance technologies and tools to help ensure the resilience and security of critical integrated grid infrastructures and would establish a Critical Infrastructure Test Facility. *The amendment was agreed to by a voice vote.*

Chairwoman Johnson moved that the Committee favorably report the bill, H.R. 5760, as amended, to the House of Representatives with the recommendation that the bill be approved. *The motion was agreed to by a voice vote.*

VI. SUMMARY OF MAJOR PROVISIONS OF THE BILL

The Grid Security Research and Development Act (H.R. 5760) would authorize a cross-agency research, development, and demonstration program to advance cyber and physical security capabilities for the energy sector at DOE, DHS, NIST, and NSF. The bill also authorizes DOE to develop technologies to enhance the resilience of the electric grid and to improve relevant emergency response and management activities, establishes a DOE critical infrastructure test facility, and requires DOE to work with stakeholders to update relevant cybersecurity roadmaps and provide guidance on implementation of cybersecurity practices, and supports the development of a cybersecurity workforce by authorizing DOE to work with relevant federal agencies and institutions of higher education to develop cybersecurity education and training.

VII. SECTION-BY-SECTION ANALYSIS (BY TITLE AND SECTION)

Sec. 1. Short title

“Grid Security Research and Development Act”

Sec. 2. Findings

Outlines the bill's findings.

*Sec. 3. Amendment to Energy Independence and Security Act of 2007**Energy Sector Security Research, Development, and Demonstration Program*

Authorizes DOE to support research, development, and demonstration activities to advance relevant cybersecurity technologies; authorizes NSF to support fundamental research to advance the cybersecurity of information systems and to support education and training for the information systems cybersecurity workforce; and authorizes DHS to identify and adapt cybersecurity tools used in the defense industry for application in the civilian energy sector.

Grid resilience and emergency response

This section authorizes a research, development, and demonstration program at DOE on methods, tools, and technologies to improve grid resilience, grid reliability, and emergency response, including technologies to detect sparks causing wildfires and assessments to determine necessary grid infrastructure upgrades. This section also authorizes a technical assistance program for eligible entities to develop plans for preventing and recovering from various power outage scenarios.

Best practices and guidance documents for energy sector cybersecurity research

This section authorizes DOE to work with stakeholders to update relevant cybersecurity roadmaps and reports; develop voluntary guidance on digital forensic analysis; and develop a mechanism to anonymize and share testing results from cybersecurity test beds. This section also authorizes NIST to work with stakeholders to develop consensus-based best practices to improve cybersecurity and to recommend cybersecurity requirements for the private sector to design and build cybersecurity into grid technologies.

Vulnerability testing and technical assistance to improve cybersecurity

Authorizes DOE to assist entities in developing cybersecurity testing capabilities; collaborate with stakeholders to evaluate cybersecurity issues and challenges in the energy sector and facilitate information sharing; and collaborate with tribal governments to improve the cybersecurity of energy assets within their jurisdiction.

Education and workforce training research and standards

Authorizes DOE to support the development of a cybersecurity workforce in collaboration with the private sector and other federal agencies, and to maintain a public database of cybersecurity education, training, and certification programs.

Interagency coordination and strategic plan for energy sector cybersecurity research

Directs DOE to develop an Interagency Strategic Plan to identify how the current work of federal agencies complements and ad-

vances the goals of the energy sector's cybersecurity research roadmap, and to make recommendations for future research.

Report to Congress

Directs DOE to submit a report to Congress that provides recommendations for additional research, development, demonstration, and commercial application activities to improve physical and cyber security of the energy sector, including the analysis of past physical- and cyber-attacks and common factors amongst attacks.

Definitions

Defines terms used in the bill.

Authorization of appropriations

Authorizes 5% annual funding increases over 5 years for grid security research, development, and demonstration activities, beginning with \$150 million in fiscal year 2021, to carry out the Act.

Sec. 4. Critical infrastructure research and construction

Directs DOE to carry out a program of research, development, and demonstration of technologies and tools to help ensure the resilience and security of critical integrated grid infrastructures, and to establish and operate a critical infrastructure test facility that allows for scalable physical and cyber performance testing to be conducted on industry-scale critical infrastructure systems.

VIII. COMMITTEE VIEWS

The Committee intends that DOE coordinate across all relevant program offices, including the DOE Office of Science in carrying out research on the topics authorized in this bill, given the need for improved cyber and physical security for the variety of technologies used in the energy sector.

IX. COST ESTIMATE

Pursuant to clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

X. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, March 12, 2020.

Hon. EDDIE BERNICE JOHNSON,
Chairman, Committee on Science, Space, and Technology,
House of Representatives, Washington, DC.

DEAR MADAM CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5760, the Grid Security Research and Development Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Sofia Guo.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

H.R. 5760, Grid Security Research and Development Act			
As ordered reported by the House Committee on Science, Space, and Technology on February 12, 2020			
By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	573	829
Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2031?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

H.R. 5760 would require the Department of Energy to administer several grant programs to advance cybersecurity, physical security, resilience, and emergency response efforts across the energy sector. The bill would authorize the appropriation of specific amounts for those purposes for each year from 2021 through 2025.

Assuming appropriation of the authorized amounts and based on spending patterns for similar activities, CBO estimates that implementing H.R. 5760 would cost \$573 million over the 2020–2025 period and \$256 million after 2025.

The costs of the legislation (detailed in Table 1) fall under budget function 270 (energy).

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 5760

	By fiscal year, millions of dollars—						
	2020	2021	2022	2023	2024	2025	2020–2025
Authorization	0	150	158	165	174	182	829
Estimated Outlays	0	34	92	126	154	167	573

The CBO staff contact for this estimate is Sofia Guo. The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

XI. FEDERAL MANDATES STATEMENT

H.R. 5760 contains no unfunded mandates.

XII. COMMITTEE OVERSIGHT FINDINGS AND RECOMMENDATIONS

The Committee's oversight findings and recommendations are reflected in the body of this report.

XIII. STATEMENT ON GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause (3)(c) of House rule XIII, the goals of H.R. 5760 are to direct Federal research on tools and technologies to advance the physical and cyber security of the energy sector, including through the development of relevant cybersecurity roadmaps and through development of a cybersecurity workforce.

XIV. FEDERAL ADVISORY COMMITTEE STATEMENT

H.R. 5760 does not authorize any federal advisory committees.

XV. DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII of the Rules of the House of Representatives, the Committee finds that no provision of H.R. 5760 establishes or reauthorizes a program of the federal government known to be duplicative of another federal program, including any program that was included in a report to Congress pursuant to section 21 of Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

XVI. EARMARK IDENTIFICATION

Pursuant to clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 5760 contains no earmarks, limited tax benefits, or limited tariff benefits.

XVII. APPLICABILITY TO THE LEGISLATIVE BRANCH

The Committee finds that H.R. 5760 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act (Public Law 104–1).

XVIII. STATEMENT ON PREEMPTION OF STATE, LOCAL, OR TRIBAL LAW

This bill is not intended to preempt any state, local, or tribal law.

XIX. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italics and existing law in which no change is proposed is shown in roman):

ENERGY INDEPENDENCE AND SECURITY ACT OF 2007

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE.**—This Act may be cited as the “Energy Independence and Security Act of 2007”.

(b) **TABLE OF CONTENTS.**—The table of contents of this Act is as follows:

Sec. 1. Short title; table of contents.

* * * * *

TITLE XIII—SMART GRID

Sec. 1301. Statement of policy on modernization of electricity grid.

- * * * * *
- Sec. 1310. *Energy sector security research, development, and demonstration program.*
- Sec. 1311. *Grid resilience and emergency response.*
- Sec. 1312. *Best practices and guidance documents for energy sector cybersecurity research.*
- Sec. 1313. *Vulnerability testing and technical assistance to improve cybersecurity.*
- Sec. 1314. *Education and workforce training research and standards.*
- Sec. 1315. *Interagency coordination and strategic plan for energy sector cybersecurity research.*
- Sec. 1316. *Report to Congress.*
- Sec. 1317. *Definitions.*
- Sec. 1318. *Authorization of appropriations.*
- * * * * *

TITLE XIII—SMART GRID

* * * * *

SEC. 1310. ENERGY SECTOR SECURITY RESEARCH, DEVELOPMENT, AND DEMONSTRATION PROGRAM.

(a) *IN GENERAL.*—The Secretary, in coordination with appropriate Federal agencies, the Electricity Subsector Coordinating Council, the Electric Reliability Organization, State, tribal, local, and territorial governments, the private sector, and other relevant stakeholders, shall carry out a research, development, and demonstration program to protect the electric grid and energy systems, including assets connected to the distribution grid, from cyber and physical attacks by increasing the cyber and physical security capabilities of the energy sector and accelerating the development of relevant technologies and tools.

(b) *DEPARTMENT OF ENERGY.*—As part of the initiative described in subsection (a), the Secretary shall award research, development, and demonstration grants to—

(1) *identify cybersecurity risks to information systems within, and impacting, the electricity sector, energy systems, and energy infrastructure;*

(2) *develop methods and tools to rapidly detect cyber intrusions and cyber incidents, including through the use of data and big data analytics techniques, such as intrusion detection, and security information and event management systems, to validate and verify system behavior;*

(3) *assess emerging cybersecurity capabilities that could be applied to energy systems and develop technologies that integrate cybersecurity features and procedures into the design and development of existing and emerging grid technologies, including renewable energy, storage, and demand-side management technologies;*

(4) *identify existing vulnerabilities in intelligent electronic devices, advanced analytics systems, and information systems;*

(5) *work with relevant entities to develop technologies or concepts that build or retrofit cybersecurity features and procedures into—*

(A) *information and energy management system devices, components, software, firmware, and hardware, including*

distributed control and management systems, and building management systems;

(B) data storage systems, data management systems, and data analysis processes;

(C) automated- and manually-controlled devices and equipment for monitoring and stabilizing the electric grid;

(D) technologies used to synchronize time and develop guidance for operational contingency plans when time synchronization technologies, are compromised;

(E) power system delivery and end user systems and devices that connect to the grid, including—

(i) meters, phasor measurement units, and other sensors;

(ii) distribution automation technologies, smart inverters, and other grid control technologies;

(iii) distributed generation, energy storage, and other distributed energy technologies;

(iv) demand response technologies;

(v) home and building energy management and control systems;

(vi) electric and plug-in hybrid vehicles and electric vehicle charging systems; and

(vii) other relevant devices, software, firmware, and hardware; and

(F) the supply chain of electric grid management system components;

(6) develop technologies that improve the physical security of information systems, including remote assets;

(7) integrate human factors research into the design and development of advanced tools and processes for dynamic monitoring, detection, protection, mitigation, response, and cyber situational awareness;

(8) evaluate and understand the potential consequences of practices used to maintain the cybersecurity of information systems and intelligent electronic devices;

(9) develop or expand the capabilities of existing cybersecurity test beds to simulate impacts of cyber attacks and combined cyber-physical attacks on information systems and electronic devices, including by increasing access to existing and emerging test beds for cooperative utilities, utilities owned by a political subdivision of a State, such as municipally-owned electric utilities, and other relevant stakeholders; and

(10) develop technologies that reduce the cost of implementing effective cybersecurity technologies and tools, including updates to these technologies and tools, in the energy sector.

(c) NATIONAL SCIENCE FOUNDATION.—The National Science Foundation, in coordination with other Federal agencies as appropriate, shall through its cybersecurity research and development programs—

(1) support basic research to advance knowledge, applications, technologies, and tools to strengthen the cybersecurity of information systems, including electric grid and energy systems, including interdisciplinary research in—

(A) evolutionary systems, theories, mathematics, and models;

(B) economic and financial theories, mathematics, and models; and

(C) big data analytical methods, mathematics, computer coding, and algorithms; and

(2) support cybersecurity education and training focused on information systems for the electric grid and energy workforce, including through the Advanced Technological Education program, the Cybercorps program, graduate research fellowships, and other appropriate programs.

(d) **DEPARTMENT OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY DIRECTORATE.**—The Science and Technology Directorate of the Department of Homeland Security shall coordinate with the Department of Energy, the private sector, and other relevant stakeholders, to research existing cybersecurity technologies and tools used in the defense industry in order to—

(1) identify technologies and tools that may meet civilian energy sector cybersecurity needs;

(2) develop a research strategy that incorporates human factors research findings to guide the modification of defense industry cybersecurity tools for use in the civilian sector;

(3) develop a strategy to accelerate efforts to bring modified defense industry cybersecurity tools to the civilian market; and

(4) carry out other activities the Secretary of Homeland Security considers appropriate to meet the goals of this subsection.

SEC. 1311. GRID RESILIENCE AND EMERGENCY RESPONSE.

(a) **IN GENERAL.**—Not later than 180 days after the enactment of the Grid Security Research and Development Act, the Secretary shall establish a research, development, and demonstration program to enhance resilience and strengthen emergency response and management pertaining to the energy sector.

(b) **GRANTS.**—The Secretary shall award grants to eligible entities under subsection (c) on a competitive basis to conduct research and development with the purpose of improving the resilience and reliability of electric grid by—

(1) developing methods to improve community and governmental preparation for and emergency response to large-area, long-duration electricity interruptions, including through the use of energy efficiency, storage, and distributed generation technologies;

(2) developing tools to help utilities and communities ensure the continuous delivery of electricity to critical facilities;

(3) developing tools to improve coordination between utilities and relevant Federal agencies to enable communication, information-sharing, and situational awareness in the event of a physical or cyber-attack on the electric grid;

(4) developing technologies and capabilities to withstand and address the current and projected impact of the changing climate on energy sector infrastructure, including extreme weather events and other natural disasters;

(5) developing technologies capable of early detection of malfunctioning electrical equipment on the transmission and distribution grid, including detection of spark ignition causing wildfires and risks of vegetation contact;

(6) assessing upgrades and additions needed to energy sector infrastructure due to projected changes in the energy generation mix and energy demand; and

[(7) upgrading tools used to estimate the costs of outages longer than 24 hours.]

[(8) developing tools and technologies to assist with the planning, safe execution of, and safe and timely restoration of power after emergency power shut offs, such as those conducted to reduce risks of wildfires started by grid infrastructure.]

(c) *ELIGIBLE ENTITIES.*—The entities eligible to receive grants under this section include—

- (1) an institution of higher education;
- (2) a nonprofit organization;
- (3) a National Laboratory;
- (4) a unit of State, local, or tribal government;
- (5) an electric utility or electric cooperative;
- (6) a retail service provider of electricity;
- (7) a private commercial entity;
- (8) a partnership or consortium of 2 or more entities described in subparagraphs (1) through (7); and
- (9) any other entities the Secretary deems appropriate.

(d) *RELEVANT ACTIVITIES.*—Grants awarded under subsection (b) shall include funding for research and development activities related to the purpose described in subsection (b), such as—

- (1) development of technologies to use distributed energy resources, such as solar photovoltaics, energy storage systems, electric vehicles, and microgrids, to improve grid and critical end-user resilience;
- (2) analysis of non-technical barriers to greater integration and use of technologies on the distribution grid;
- (3) analysis of past large-area, long-duration electricity interruptions to identify common elements and best practices for electricity restoration, mitigation, and prevention of future disruptions;
- (4) development of advanced monitoring, analytics, operation, and controls of electric grid systems to improve electric grid resilience;
- (5) analysis of technologies, methods, and concepts that can improve community resilience and survivability of frequent or long-duration power outages;
- (6) development of methodologies to maintain cybersecurity during restoration of energy sector infrastructure and operation;
- (7) development of advanced power flow control systems and components to improve electric grid resilience; and
- (8) any other relevant activities determined by the Secretary.

(e) *TECHNICAL ASSISTANCE.*—

(1) *IN GENERAL.*—The Secretary shall provide technical assistance to eligible entities for the commercial application of technologies to improve the resilience of the electric grid and commercial application of technologies to help entities develop plans for preventing and recovering from various power outage scenarios at the local, regional, and State level.

(2) *TECHNICAL ASSISTANCE PROGRAM.*—The commercial application technical assistance program established in paragraph (1) shall include assistance to eligible entities for—

(A) the commercial application of technologies developed from the grant program established in subsection (b), including cooperative utilities and utilities owned by a political subdivision of a State, such as municipally-owned electric utilities;

(B) the development of methods to strengthen or otherwise mitigate adverse impacts on electric grid infrastructure against natural hazards;

(C) the use of Department data and modeling tools for various purposes;

(D) a resource assessment and analysis of future demand and distribution requirements, including development of advanced grid architectures and risk analysis; and

(E) the development of tools and technologies to coordinate data across relevant entities to promote resilience and wildfire prevention in the planning, design, construction, operation, and maintenance of transmission infrastructure;

(F) analysis to predict the likelihood of extreme weather events to inform the planning, design, construction, operation, and maintenance of transmission infrastructure in consultation with the National Oceanic and Atmospheric Administration; and

(G) the commercial application of relevant technologies, such as distributed energy resources, microgrids, or other energy technologies, to establish backup power for users or facilities affected by emergency power shutoffs.

(3) **ELIGIBLE ENTITIES.**—The entities eligible to receive technical assistance for commercial application of technologies under this section include—

(A) representatives of all sectors of the electric power industry, including electric utilities, trade organizations, and transmission and distribution system organizations, owners, and operators;

(B) State and local governments and regulatory authorities, including public utility commissions;

(C) tribal and Alaska Native governmental entities;

(D) partnerships among entities under subparagraphs (A) through (C);

(E) regional partnerships; and

(F) any other entities the Secretary deems appropriate.

(4) **AUTHORITY.**—Nothing in this section shall authorize the Secretary to require any entity to adopt any model, tool, technology, plan, analysis, or assessment.

SEC. 1312. BEST PRACTICES AND GUIDANCE DOCUMENTS FOR ENERGY SECTOR CYBERSECURITY RESEARCH.

(a) **IN GENERAL.**—The Secretary, in coordination with appropriate Federal agencies, the Electricity Subsector Coordinating Council, standards development organizations, State, tribal, local, and territorial governments, the private sector, public utility commissions, and other relevant stakeholders, shall coordinate the development of guidance documents for research, development, and demonstration activities to improve the cybersecurity capabilities of the energy sector through participating agencies. As part of these activities, the Secretary shall—

(1) facilitate stakeholder involvement to update—

- (A) *the Roadmap to Achieve Energy Delivery Systems Cybersecurity;*
- (B) *the Cybersecurity Procurement Language for Energy Delivery Systems, including developing guidance for—*
 - (i) *contracting with third parties to conduct vulnerability testing for information systems used across the energy production, delivery, storage, and end use systems;*
 - (ii) *contracting with third parties that utilize transient devices to access information systems; and*
 - (iii) *managing supply chain risks; and*
- (C) *the Electricity Subsector Cybersecurity Capability Maturity Model, including the development of metrics to measure changes in cybersecurity readiness; and*
- (2) *develop voluntary guidance to improve digital forensic analysis capabilities, including—*
 - (A) *developing standardized terminology and monitoring processes; and*
 - (B) *utilizing human factors research to develop more effective procedures for logging incident events; and*
- (3) *work with the National Science Foundation, Department of Homeland Security, and stakeholders to develop a mechanism to anonymize, aggregate, and share the testing results from cybersecurity test beds to facilitate technology improvements by public and private sector researchers.*
- (b) *BEST PRACTICES.—The Secretary, in collaboration with the Director of the National Institute of Standards and Technology and other appropriate Federal agencies, shall convene relevant stakeholders and facilitate the development of—*
 - (1) *consensus-based best practices to improve cybersecurity for—*
 - (A) *emerging energy technologies;*
 - (B) *distributed generation and storage technologies, and other distributed energy resources;*
 - (C) *electric vehicles and electric vehicle charging stations; and*
 - (D) *other technologies and devices that connect to the electric grid;*
 - (2) *recommended cybersecurity designs and technical requirements that can be used by the private sector to design and build interoperable cybersecurity features into technologies that connect to the electric grid, including networked devices and components on distribution systems; and*
 - (3) *technical analysis that can be used by the private sector in developing best practices for test beds and test bed methodologies that will enable reproducible testing of cybersecurity protections for information systems, electronic devices, and other relevant components, software, and hardware across test beds.*
- (c) *REGULATORY AUTHORITY.—None of the activities authorized in this section shall be construed to authorize regulatory actions. Additionally, the voluntary standards developed under this section shall not duplicate or conflict with mandatory reliability standards.*

SEC. 1313. VULNERABILITY TESTING AND TECHNICAL ASSISTANCE TO IMPROVE CYBERSECURITY.

(a) *IN GENERAL.*—*The Secretary shall—*

(1) *coordinate with energy sector asset owners and operators, leveraging the research facilities and expertise of the National Laboratories, to assist entities in developing testing capabilities by—*

(A) *utilizing a range of methods to identify vulnerabilities in physical and cyber systems;*

(B) *developing cybersecurity risk assessment tools and providing analyses and recommendations to participating stakeholders; and*

(C) *working with stakeholders to develop methods to share anonymized and aggregated test results to assist relevant stakeholders in the energy sector, researchers, and the private sector to advance cybersecurity efforts, technologies, and tools;*

(2) *collaborate with relevant stakeholders, including public utility commissions, to—*

(A) *identify information, research, staff training, and analytical tools needed to evaluate cybersecurity issues and challenges in the energy sector; and*

(B) *facilitate the sharing of information and the development of tools identified under subparagraph (A);*

(3) *collaborate with tribal governments to identify information, research, and analysis tools needed by tribal governments to increase the cybersecurity of energy assets within their jurisdiction.*

SEC. 1314. EDUCATION AND WORKFORCE TRAINING RESEARCH AND STANDARDS.

(a) *IN GENERAL.*—*The Secretary shall support the development of a cybersecurity workforce through a program that—*

(1) *facilitates collaboration between undergraduate and graduate students, researchers at the National Laboratories, and the private sector;*

(2) *prioritizes science and technology in areas relevant to the mission of the Department of Energy through the design and application of cybersecurity technologies;*

(3) *develops, or facilitates private sector development of, voluntary cybersecurity training and retraining standards, lessons, and recommendations for the energy sector that minimize duplication of cybersecurity compliance training programs; and*

(4) *maintains a public database of cybersecurity education, training, and certification programs.*

(b) *GRID RESILIENCE TECHNOLOGY TRAINING.*—*The Secretary shall support the development of the grid workforce through a training program that prioritizes activities that enhance the resilience of the electric grid and energy sector infrastructure, including training on the use of tools, technologies, and methods developed under the grant program established in section 1311(b).*

(c) *COLLABORATION.*—*In carrying out the program authorized in subsection (a) and (b), the Secretary shall leverage programs and activities carried out across the Department of Energy, other relevant Federal agencies, institutions of higher education, and other*

appropriate entities best suited to provide national leadership on cybersecurity and grid resilience-related issues.

SEC. 1315. INTERAGENCY COORDINATION AND STRATEGIC PLAN FOR ENERGY SECTOR CYBERSECURITY RESEARCH.

(a) DUTIES.—The Secretary, in coordination with the Energy Sector Government Coordinating Council, shall—

(1) review the most recent versions of the Roadmap to Achieve Energy Delivery Systems Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity to identify cross-cutting energy sector cybersecurity research needs and opportunities for collaboration among Federal agencies and other relevant stakeholders;

(2) identify interdisciplinary research, technology, and tools that can be applied to cybersecurity challenges in the energy sector;

(3) identify technology transfer opportunities to accelerate the development and commercial application of novel cybersecurity technologies, systems, and processes in the energy sector; and

(4) develop a coordinated Interagency Strategic Plan for research to advance cybersecurity capabilities used in the energy sector that builds on the Roadmap to Achieve Energy Delivery Systems in Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity.

(b) INTERAGENCY STRATEGIC PLAN.—

(1) SUBMITTAL.—The Interagency Strategic Plan developed under subsection (a)(4) shall be submitted to Congress and made public within 12 months after the date of enactment of the Grid Security Research and Development Act.

(2) CONTENTS.—The Interagency Strategic Plan shall include—

(A) an analysis of how existing cybersecurity research efforts across the Federal Government are advancing the goals of the Roadmap to Achieve Energy Delivery Systems Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity;

(B) recommendations for research areas that may advance the cybersecurity of the energy sector;

(C) an overview of existing and proposed public and private sector research efforts that address the topics outlined in paragraph (3); and

(D) an overview of needed support for workforce training in cybersecurity for the energy sector.

(3) CONSIDERATIONS.—In developing the Interagency Strategic Plan, the Secretary, in coordination with the Energy Sector Government Coordinating Council, shall consider—

(A) opportunities for human factors research to improve the design and effectiveness of cybersecurity devices, technologies, tools, processes, and training programs;

(B) contributions of other disciplines to the development of innovative cybersecurity procedures, devices, components, technologies, and tools;

(C) opportunities for technology transfer programs to facilitate private sector development of cybersecurity procedures, devices, components, technologies, and tools for the energy sector;

(D) broader applications of the work done by relevant Federal agencies to advance the cybersecurity of information systems and data analytics systems for the energy sector; and

(E) activities called for in the Federal cybersecurity research and development strategic plan required by section 201(a)(1) of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7431(a)(1)).

(c) **PARTICIPATION.**—For the purposes of carrying out this section, the Energy Sector Government Coordinating Council shall include representatives from Federal agencies with expertise in the energy sector, information systems, data analytics, cyber and physical systems, engineering, human factors research, human-machine interfaces, high performance computing, big data and data analytics, or other disciplines considered appropriate by the Council Chair.

SEC. 1316. REPORT TO CONGRESS.

(a) **BALANCING RISKS, INCREASING SECURITY, AND IMPROVING MODERNIZATION.**—

(1) **STUDY.**—The Secretary, in collaboration with the National Institute of Standards and Technology, other Federal agencies, and energy sector stakeholders, in order to provide recommendations for additional research, development, demonstration, and commercial application activities, shall—

(A) analyze physical and cyber attacks on energy sector infrastructure and information systems and identify cost-effective opportunities to improve physical and cyber security; and

(B) examine the risks associated with increasing penetration of digital technologies in grid networks, particularly on the distribution grid.

(2) **CONTENT.**—The study shall—

(A) analyze processes, operational procedures, and other factors common among cyber attacks;

(B) identify areas where human behavior plays a critical role in maintaining or compromising the security of a system;

(C) recommend—

(i) changes to the design of devices, human-machine interfaces, technologies, tools, processes, or procedures to optimize security that do not require a change in human behavior; and

(ii) training techniques to increase the capacity of employees to actively identify, prevent, or neutralize the impact of cyber attacks;

(D) evaluate existing engineering and technical design criteria and guidelines that incorporate human factors research findings, and recommend criteria and guidelines for cybersecurity tools that can be used to develop display systems for cybersecurity monitoring, such as alarms, user-friendly displays, and layouts;

(E) evaluate the cybersecurity risks and benefits of various design and architecture options for energy sector systems, networked grid systems and components, and automation systems, including consideration of—

(i) designs that include both digital and analog control devices and technologies;

(ii) different communication technologies used to transfer information and data between control system devices, technologies, and system operators;

(iii) automated and human-in-the-loop devices and technologies;

(iv) programmable versus nonprogrammable devices and technologies;

(v) increased redundancy using dissimilar cybersecurity technologies; and

(vi) grid architectures that use autonomous functions to limit control vulnerabilities; and

(F) recommend methods or metrics to document changes in risks associated with system designs and architectures.

(3) *CONSULTATION.*—In conducting the study, the Secretary shall consult with energy sector stakeholders, academic researchers, the private sector, and other relevant stakeholders.

(4) *REPORT.*—Not later than 24 months after the date of enactment of the Grid Security Research and Development Act, the Secretary shall submit the study to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Energy and Natural Resources of the Senate.

SEC. 1317. DEFINITIONS.

In this title:

(1) *BIG DATA.*—The term “big data” means datasets that require advanced analytical methods for their transformation into useful information.

(2) *CYBERSECURITY.*—The term “cybersecurity” means protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(3) *CYBERSECURITY THREAT.*—The term “cybersecurity threat” has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(4) *ELECTRICITY SUBSECTOR COORDINATING COUNCIL.*—The term “Electricity Subsector Coordinating Council” means the self-organized, self-governed council consisting of senior industry representatives to serve as the principal liaison between the Federal Government and the electric power sector and to carry out the role of the Sector Coordinating Council as established in the National Infrastructure Protection Plan for the electricity subsector.

(5) *ENERGY SECTOR GOVERNMENT COORDINATING COUNCIL.*—The term “Energy Sector Government Coordinating Council” means the council consisting of representatives from relevant Federal Government agencies to provide effective coordination of energy sector efforts to ensure a secure, reliable, and resilient energy infrastructure and to carry out the role of the Government Coordinating Council as established in the National Infrastructure Protection Plan for the energy sector.

(6) *HUMAN FACTORS RESEARCH.*—The term “human factors research” means research on human performance in social and physical environments, and on the integration and interaction

of humans with physical systems and computer hardware and software.

(7) *HUMAN-MACHINE INTERFACES.*—The term “human-machine interfaces” means technologies that present information to an operator or user about the state of a process or system, or accept human instructions to implement an action, including visualization displays such as a graphical user interface.

(8) *INFORMATION SYSTEM.*—The term “information system”—

(A) has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and

(B) includes operational technology, information technology, and communications.

(9) *NATIONAL LABORATORY.*—The term “national laboratory” has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(10) *SECURITY VULNERABILITY.*—The term “security vulnerability” has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(11) *TRANSIENT DEVICES.*—The term “transient devices” means removable media, including floppy disks, compact disks, USB flash drives, external hard drives, mobile devices, and other devices that utilize wireless connections.

SEC. 1318. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Secretary to carry out this Act—

- (1) \$150,000,000 for fiscal year 2021;
- (2) \$157,500,000 for fiscal year 2022;
- (3) \$165,375,000 for fiscal year 2023;
- (4) \$173,645,000 for fiscal year 2024; and
- (5) \$182,325,000 for fiscal year 2025.

* * * * *

XX. EXCHANGE OF COMMITTEE CORRESPONDENCE

EDDIE BERNICE JOHNSON, Texas
CHAIRWOMAN

FRANK D. LUCAS, Oklahoma
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6375

www.science.house.gov

September 2, 2020

Chairman Bennie G. Thompson
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, D.C. 20515

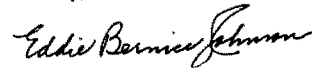
Dear Chairman Thompson,

I am writing to you concerning H.R. 5760, the "Grid Security Research and Development Act," which was referred to the Committee on Science, Space, and Technology, and in addition to the Committee on Homeland Security on February 5, 2020.

I appreciate your willingness to work cooperatively on this bill. I recognize that the bill contains provisions that fall within the jurisdiction of the Committee on Homeland Security. I appreciate that your Committee will waive further consideration of H.R. 5760 and that this action is not a waiver of future jurisdictional claims by the Committee on Homeland Security over this subject matter.

I will make sure to include our exchange of letters in the legislative report for H.R. 5760 and in the *Congressional Record*. Thank you for your cooperation on this legislation.

Sincerely,



Eddie Bernice Johnson
Chairwoman
Committee on Science, Space, and Technology

cc:

Ranking Member Frank D. Lucas, Committee on Science, Space, and Technology
Ranking Member Mike Rogers, Committee on Homeland Security
Tom Wickham, Parliamentarian

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN



MIKE ROGERS, ALABAMA
RANKING MEMBER

One Hundred Sixteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

September 2, 2020

The Honorable Eddie Bernice Johnson
Chairwoman
Committee on Science, Space and Technology
2321 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

Dear Chairwoman Johnson:

I write to you regarding H.R. 5760, the "Grid Security Research and Development Act."

H.R. 5760 contains provisions that fall within the jurisdiction of the Committee on Homeland Security. I recognize and appreciate your desire to see this legislation implemented and accordingly, I will not seek a sequential referral of the bill. However, agreeing to waive consideration of this bill should not be construed as the Committee on Homeland Security waiving, altering, or otherwise affecting its jurisdiction over subject matters contained in the bill which fall within its Rule X jurisdiction.

I would also ask that a copy of this letter and your response be included in the legislative report on H.R. 5760 and in the *Congressional Record* during any future floor consideration of this bill.

I look forward to working with you on this and other important legislation in the future.

Sincerely,


BENNIE G. THOMPSON
Chairman

cc: The Honorable Nancy Pelosi, Speaker
The Honorable Michael Rogers, Ranking Member
The Honorable Tom Wickham, Parliamentarian

XXI. PROCEEDINGS OF THE FULL COMMITTEE MARKUP

MARKUPS:
H.R. 2986, THE BETTER ENERGY STORAGE
TECHNOLOGY (BEST) ACT;
H.R. 4230, THE CLEAN INDUSTRIAL
TECHNOLOGY (CIT) ACT OF 2019;
H.R. 5374, THE ADVANCED GEOTHERMAL
RESEARCH AND DEVELOPMENT ACT OF 2019;
H.R. 5428, THE GRID MODERNIZATION
RESEARCH AND DEVELOPMENT
ACT OF 2019; AND
H.R. 5760, THE GRID SECURITY RESEARCH
AND DEVELOPMENT ACT

MARKUP

BEFORE THE

COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

FEBRUARY 12, 2020

Serial No. CP: 116-15

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE
WASHINGTON : 2020

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. EDDIE BERNICE JOHNSON, Texas, *Chairwoman*

ZOE LOFGREN, California
 DANIEL LIPINSKI, Illinois
 SUZANNE BONAMICI, Oregon
 AMI BERA, California,

Vice Chair

CONOR LAMB, Pennsylvania
 LIZZIE FLETCHER, Texas
 HALEY STEVENS, Michigan
 KENDRA HORN, Oklahoma
 MIKIE SHERRILL, New Jersey
 BRAD SHERMAN, California
 STEVE COHEN, Tennessee
 JERRY MCNERNEY, California
 ED PERLMUTTER, Colorado
 PAUL TONKO, New York
 BILL FOSTER, Illinois
 DON BEYER, Virginia
 CHARLIE CRIST, Florida
 SEAN CASTEN, Illinois
 BEN McADAMS, Utah
 JENNIFER WEXTON, Virginia
 CONOR LAMB, Pennsylvania
 VACANCY

FRANK D. LUCAS, Oklahoma,
Ranking Member
 MO BROOKS, Alabama
 BILL POSEY, Florida
 RANDY WEBER, Texas
 BRIAN BABIN, Texas
 ANDY BIGGS, Arizona
 ROGER MARSHALL, Kansas
 RALPH NORMAN, South Carolina
 MICHAEL CLOUD, Texas
 TROY BALDERSON, Ohio
 PETE OLSON, Texas
 ANTHONY GONZALEZ, Ohio
 MICHAEL WALTZ, Florida
 JIM BAIRD, Indiana
 JAIME HERRERA BEUTLER, Washington
 FRANCIS ROONEY, Florida
 GREGORY F. MURPHY, North Carolina

C O N T E N T S

Wednesday, February 12, 2020

	Page
H.R. 2986— <i>Better Energy Storage Technology Act or the BEST Act</i>	7
H.R. 4230— <i>Clean Industrial Technology Act of 2019 or CIT Act of 2019</i>	38
H.R. 5374— <i>Advanced Geothermal Research and Development Act of 2019</i>	75
H.R. 5428— <i>Grid Modernization Research and Development Act of 2019</i>	111
H.R. 5760— <i>Grid Security Research and Development Act</i>	150

**Markup on H.R. 2986,
Better Energy Storage Technology Act
or the BEST Act**

**Markup on H.R. 4230, Clean Industrial
Technology Act of 2019 or CIT Act of 2019**

**Markup on H.R. 5374,
Advanced Geothermal Research
and Development Act of 2019**

**Markup on H.R. 5428,
Grid Modernization Research
and Development Act of 2019**

**Markup on H.R. 5760,
Grid Security Research and Development Act**

WEDNESDAY, FEBRUARY 12, 2020

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, DC.

The Committee met, pursuant to notice, at 10 o'clock a.m., in room 2318 of the Rayburn House Office Building, Hon. Eddie Bernice Johnson [Chairwoman of the Committee] presiding.

Chairwoman JOHNSON. Good morning. The Committee will come to order. Without objection, the Chair is authorized to declare recess at any time. Pursuant to Committee rule and the House rules, the Chair announces that she may postpone roll call votes.

Pursuant to notice, the Committee meets to consider the following measures: H.R. 2986, *Better Energy Storage Technology Act*; H.R. 4230, *Clean Industrial Technology Act of 2019*; H.R. 5374, *Advanced Geothermal Research and Development Act of 2019*; H.R. 5428, *Grid Modernization Research and Development Act of 2019*; H.R. 5760, *Grid Security Research and Development Act*.

We welcome all to the Science Committee markup of five good, bipartisan bills. First, we will consider the *Better Energy Storage Technology Act (BEST ACT)*. The *BEST Act* authorizes the Department of Energy to conduct a crosscutting research, development, and demonstration program on energy storage technologies, including batteries and pumped hydro systems. The act requires DOE (Department of Energy) to create a 5-year strategic plan to coordinate research activities among DOE's technology offices.

Renewable energy technology can be intermittent. Strong winds die down, and sunny days turn cloudy. According to the Congressional Research Service, energy storage systems may be a key technology to enabling a reliable, low greenhouse-gas-emitting electric grid comprised of energy generation sources like wind and solar.

Next, we have H.R. 4230, the *Clean Industrial Technology Act of 2019*. The act authorizes an interagency, DOE-led research, development, and demonstration program to advance technologies that will help reduce emissions from the manufacturing sector, including steel and cement production, chemical production, and industrial heat. The research program will be carried out in collaboration with the stakeholders from industry and labor groups. Allowing American manufacturers to access technologies that make them increasingly sustainable will ensure that the domestic manufacturing industry will remain competitive throughout the 21st century.

We will then move to H.R. 5374, the *Advanced Geothermal Research and Development Act of 2019*. I will speak about this bill a little bit later.

Next is H.R. 5428, the *Grid Modernization Research and Development Act of 2019*, which authorizes a broad research, development, and demonstration program on a wide variety of topics pertaining to grid modernization, including smart grid modeling, planning, and controls; hybrid energy systems; and enhanced electric grid integration of technologies like vehicles and building components. Our Nation's electricity grid is undergoing a series of transformations, which includes adapting to a changing electricity generation mix, an increase in smart-grid technologies, and a growing need for improved resilience of the electric power grid. This bill will help lead our Nation in developing the technologies we need by setting forth a comprehensive research agenda by the DOE.

Finally, we'll be considering H.R. 5760, the *Grid Security Research and Development Act*. This bill is an updated version of a bill that Mr. Bera and I introduced, along with many of our Science Committee colleagues, in the previous two Congresses. H.R. 5760 will provide legislative guidance to activities carried out by the re-

cently established DOE Office of Cybersecurity, Energy Security, and Emergency Response. The bill authorizes an interagency research and development program to advance electric grid cybersecurity, physical security, grid resilience, and emergency response efforts. In particular, the bill authorizes activities on the cybersecurity testbeds, education and workforce training and standards, and guidance documents for energy sector cybersecurity practices.

I'm proud that today's bills are supported by a cross-section of interested groups. One or more of today's bills has been endorsed by organizations that include the National Audubon Society, the U.S. Chamber of Commerce, the Information Technology and Innovation Foundation, the Environmental Defense Fund, the National Rural Electric Cooperatives Association, Duke Energy, the Union of Concerned Scientists, the Natural Resources Defense Fund, and the National Association of Manufacturers.

Thank you.

[The statement of Chairwoman Johnson follows:]

Good morning, and welcome to today's Science Committee markup of five good, bipartisan bills.

First, we will consider H.R. 2986, the Better Energy Storage Technology Act. The BEST Act authorizes the Department of Energy to conduct a cross-cutting research, development, and demonstration program on energy storage technologies, including batteries and pumped hydro systems. The Act requires DOE create a 5-year strategic plan to coordinate research activities among DOE's technology offices.

Renewable energy technology can be intermittent. Strong winds die down, and sunny days turn cloudy. According to the Congressional Research Service, energy storage systems may be a key technology to enabling a reliable, low greenhouse gas emitting electric grid comprised of energy generation sources like wind and solar.

Next we have H.R. 4230, the Clean Industrial Technology Act of 2019. This act authorizes an intra-agency, DOE-led research, development, and demonstration program to advance technologies that will help reduce emissions from the manufacturing sector, including steel and cement production, chemical production, and industrial heat. The research program will be carried out in collaboration with stakeholders from industry and labor groups.

Allowing American manufacturers to access technologies that make them increasingly sustainable will ensure that the domestic manufacturing industry will remain competitive through the 21st Century.

We will then move on to H.R. 5374, the Advanced Geothermal Research and Development Act of 2019. I will speak about this bill a little later.

Next is H.R. 5428, the Grid Modernization Research and Development Act of 2019, which authorizes a broad research, development, and demonstration program on a wide variety of topics pertaining to grid modernization, including smart grid modeling, planning, and controls; hybrid energy systems; and enhanced electric grid integration of technologies like vehicles and building components.

Our nation's electricity grid is undergoing a series of transformations, which include adapting to a changing electricity generation mix, an increase in "smart grid" technologies, and a growing need to improve the resilience of the electric power grid. This bill will help lead our nation in developing the technologies we need by setting forth a comprehensive research agenda led by the DOE.

Finally, we'll be considering H.R. 5760, the Grid Security Research and Development Act. This bill is an updated version of a bill that Mr. Bera and I introduced, along with many of our Science Committee colleagues, in the previous two Congresses.

H.R. 5760 will provide legislative guidance to the activities carried out by the recently established DOE Office of Cybersecurity, Energy Security, and Emergency Response. The bill authorizes an interagency research and development program to advance electric grid cybersecurity, physical security, grid resilience, and emergency response efforts. In particular, the bill authorizes activities on cybersecurity testbeds, education and workforce training and standards, and guidance documents for energy sector cybersecurity practices.

I am proud that today's bills are supported by a cross-section of interested groups. One or more of today's bills has been endorsed by organizations that include: the

National Audubon Society, the U.S. Chamber of Commerce, the Information Technology & Innovation Foundation (ITIF), the Environmental Defense Fund (EDF), the National Rural Electric Cooperative Association, Duke Energy, the Union of Concerned Scientists, the Natural Resources Defense Fund, and the National Association of Manufacturers.

Chairwoman JOHNSON. I now recognize our Ranking Member for his opening remarks.

Mr. LUCAS. Thank you, Chairwoman Johnson, for holding today's full Committee markup.

The Science Committee has one of the best records in Congress for passing productive, bipartisan legislation, and I'm very pleased to see us upholding that tradition this morning. We've reached bipartisan agreement on the five energy bills being considered today.

Currently, the U.S. energy sector faces a number of critical challenges, and it can be difficult to find the best path forward in a world that increasingly demands cleaner, more reliable, and more affordable energy sources. But it is our job in Congress to set the priorities to address these challenges and focus our limited Federal resources where we can see the best return on investment.

To deliver truly effective solutions, we must take the long-term and big-picture approach. We must support research in fundamental science that drives innovation over a broad range of energy applications and strategically invest in the early stage clean-energy technologies that industry cannot support. We must also provide for R&D (research and development) to modernize and defend our critical energy infrastructure and address the complex energy needs of our Nation's industrial sectors. These are the initiatives that today's bills will address.

First, we'll consider this morning H.R. 2986, the *BEST Energy Storage Technology Act of 2019*. This legislation authorizes a cross-cutting research and development program at the Department of Energy to provide necessary direction on high-priority energy storage technology research and development activities. Advanced grid scale energy storage is an essential component of any comprehensive clean-energy strategy and a priority of the current Administration. Developing our grid scale energy storage ability will accelerate the growth in all kinds of energy production, which can make use of this technology.

Our second bill this morning is H.R. 4230, the *Clean Industrial Technology Act of 2019*. Our Nation's economic stability and national security are tied to the growth of the U.S. industrial sector, yet the demanding energy needs of industry can represent a unique challenge for our clean and secure future energy. This bill establishes a DOE program to support the development of innovative technologies and practices that will reduce industrial sector emissions while maintaining the effectiveness and competitiveness of U.S. industry. It also requires the Secretary to establish a comprehensive strategy to develop the mission and goals for this new program.

While I can't say I agree with every aspect of this legislation, I'd like to thank our friends across the aisle for meeting us at the table to come to an agreement. By having a good-faith discussion, we were able to add responsible funding levels and good governance provisions to H.R. 4230 that will make this legislation a bipartisan product.

Next, we'll consider my bill, H.R. 5374, the *Advanced Geothermal Research and Development Act of 2019*, which authorizes DOE's cutting-edge geothermal research and development activities. This bill establishes a geothermal computing program and includes funding for critical geothermal user facilities that will support the next generation of electricity generation from these vast and largely untapped renewable resources. I would like to thank Chairwoman Johnson for cosponsoring this legislation and working with me to refine it.

While many renewables like wind and solar are already seeing success in the market, early stage technologies like geothermal, which are often far too expensive and risky for industry to take to scale, require Federal support for R&D. By strategically investing in these promising technologies, we can continue to enhance our diverse domestic energy portfolio and bolster U.S. energy independence. While we support next-generation energy technologies and clean-energy strategies, we must also increase our investment in our critical energy infrastructure.

So, finally, the Committee will consider H.R. 5428, the *Grid Modernization Research and Development Act of 2019*, and H.R. 5760, the *Grid Security Research and Development Act*. Together, these two bills authorize DOE's critical work in strengthening our Nation's electric grid against rapidly changing technological challenges. The *Grid Security Research and Development Act* authorizes the Department's critical cybersecurity and emergency response R&D activities and directs DOE to work with relevant Federal agencies to develop cybersecurity best practices. The *Grid Modernization Research and Development Act* authorizes R&D into hybrid energy systems, grid integration, and smart grid modeling, modernizing the grid to improve its overall resilience and flexibility.

I'd like to take this opportunity to thank my good friends across the aisle for working with us on these bills. I appreciate that we can come together to focus on our shared interest in supporting commonsense legislation to maintain U.S. national security, environmental stewardship, economic prosperity, and energy security for years to come. And I'd like to again thank Chairwoman Johnson for holding this markup, and I yield back the balance of my time.

[The statement of Mr. Lucas follows:]

Thank you, Chairwoman Johnson, for holding today's full Committee mark-up.

The Science Committee has one of the best track records in Congress for passing productive, bipartisan legislation, and I'm very pleased to see us upholding that tradition this morning. We've reached bipartisan agreement on the five energy bills being considered today.

Currently, the U.S. energy sector faces a number of critical challenges, and it can be difficult to find the best path forward in a world that increasingly demands cleaner, more reliable, and more affordable energy sources. But it is our job in Congress to set the priorities to address these challenges and focus our limited federal funds where we can see the best return on investment.

To deliver truly effective solutions, we must take the long-term and big picture approach. We must support research in fundamental science that drives innovation over a broad range of energy applications, and strategically invest in the early-stage clean energy technologies that industry cannot support. We must also provide for R&D to modernize and defend our critical energy infrastructure and address the complex energy needs of our nation's industrial sectors. These are the initiatives that today's bills will address.

The first bill we will consider this morning is H.R. 2986, the "Better Energy Storage Technology Act of 2019." This legislation authorizes a cross-cutting research and development program at the Department of Energy (DOE) to provide necessary direction on high-priority energy storage technology research and development activities.

Advanced grid scale energy storage is an essential component of any comprehensive clean energy strategy and a priority of the current administration. Developing our grid scale energy storage ability will accelerate growth in all kinds of energy production, which can make use of this technology.

Our second bill this morning is H.R. 4230, the "Clean Industrial Technology Act of 2019." Our nation's economic stability and national security are tied to the growth of the U.S. industrial sector.

Yet the demanding energy needs of industry can represent a unique challenge for our clean and secure energy future. This bill establishes a DOE program to support the development of innovative technologies and practices that will reduce industrial sector emissions while maintaining the effectiveness and competitiveness of U.S. industry. It also requires the Secretary to establish a comprehensive strategy to develop the mission and goals for this new program.

While I can't say I agree with every aspect of this legislation, I would like to thank our friends across the aisle for meeting us at the table to come to an agreement. By having a good-faith discussion, we were able to add responsible funding levels and good governance provisions to H.R. 4230 that will make this legislation a bipartisan product.

Next we will consider my bill, H.R. 5374, the "Advanced Geothermal Research and Development Act of 2019" which authorizes DOE's cutting-edge geothermal research and development activities. This bill establishes a geothermal computing program and includes funding for critical geothermal energy user facilities that will support the next generation of electricity generation from these vast and largely untapped renewable resources. I would like to thank Chairwoman Johnson for cosponsoring this legislation and for working with me to refine it.

While many renewables like wind and solar are already seeing success in the market, early stage technologies like geothermal, which are often far too expensive and risky for industry to take to scale, require federal support for R&D. By strategically investing in these promising technologies we can continue to enhance our diverse domestic energy portfolio and bolster U.S. energy independence.

While we support next-generation energy technologies and clean energy strategies, we must also increase our investment in our critical energy infrastructure. So finally, the Committee will consider H.R. 5428, the "Grid Modernization Research and Development Act of 2019" and H.R. 5760, the "Grid Security Research and Development Act."

Together, these two bills authorize DOE's critical work in strengthening our nation's electric grid against rapidly changing technological challenges. The Grid Security Research and Development Act authorizes the Department's crucial cybersecurity and emergency response R&D activities and directs DOE to work with relevant Federal agencies to develop cybersecurity best practices. The Grid Modernization Research and Development Act authorizes R&D into hybrid energy systems, grid integration, and smart grid modeling - modernizing the grid to improve its overall resilience and flexibility.

I'd like to take this opportunity to thank my good friends across the aisle for working with us on these bills. I appreciate that we can come together to focus on our shared interest in supporting commonsense legislation to maintain U.S. national security, environmental stewardship, economic prosperity, and energy security for years to come. I'd like to again thank Chairwoman Johnson for holding this markup and I yield back the balance of my time.

Chairwoman JOHNSON. Thank you very much.

38

149

We will now consider H.R. 5760, the *Grid Security Research and Development Act*. The clerk will report the bill.

The CLERK. H.R. 5760, a bill—
[The bill follows:]

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

.....
 (Original Signature of Member)

116TH CONGRESS
 1ST SESSION

H. R. _____

To provide for a comprehensive interdisciplinary research, development, and demonstration initiative to strengthen the capacity of the energy sector to prepare for and withstand cyber and physical attacks, and for other purposes.

 IN THE HOUSE OF REPRESENTATIVES

Mr. Bera (for himself and Mr. Weber) introduced the following bill; which was referred to the Committee on _____

A BILL

To provide for a comprehensive interdisciplinary research, development, and demonstration initiative to strengthen the capacity of the energy sector to prepare for and withstand cyber and physical attacks, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
 2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Grid Security Research
 5 and Development Act”.

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

2

1 **SEC. 2. FINDINGS.**

2 Congress finds the following:

3 (1) The Nation, and every critical infrastruc-
4 ture sector, depends on reliable electricity.

5 (2) Intelligent electronic devices, advanced ana-
6 lytics, and information systems used across the en-
7 ergy sector are essential to maintaining reliable op-
8 eration of the electric grid.

9 (3) The cybersecurity threat landscape is con-
10 stantly changing and attacker capabilities are ad-
11 vancing rapidly, requiring ongoing modifications, ad-
12 vancements, and investments in technologies and
13 procedures to maintain security.

14 (5) It is in the national interest for Federal
15 agencies to invest in cybersecurity research that in-
16 forms and facilitates private sector investment and
17 use of advanced cybersecurity tools and procedures
18 to protect information systems.

19 (6) The number of devices and systems con-
20 necting to the electric grid is increasing, and inte-
21 grating cybersecurity protections into information
22 systems when they are built is more effective than
23 modifying products after installation to meet cyber-
24 security goals.

25 (7) An understanding of human factors can be
26 leveraged to understand the behavior of cyber threat

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

1 actors, develop strategies to counter threat actors,
2 improve cybersecurity training programs, optimize
3 the design of human-machine interfaces and cyberse-
4 curity tools, and increase the capacity of the energy
5 sector workforce to prevent unauthorized access to
6 critical systems.

7 **SEC. 3. AMENDMENT TO ENERGY INDEPENDENCE AND SE-**
8 **CURITY ACT OF 2007.**

9 Title XIII of the Energy Independence and Security
10 Act of 2007 (42 U.S.C. 17381 et seq.) is amended by add-
11 ing at the end the following:

12 **“SEC. 1310. ENERGY SECTOR SECURITY RESEARCH, DEVEL-**
13 **OPMENT, AND DEMONSTRATION PROGRAM.**

14 “(a) IN GENERAL.—The Secretary, in coordination
15 with appropriate Federal agencies, the Electricity Sub-
16 sector Coordinating Council, the Electric Reliability Orga-
17 nization, State, tribal, local, and territorial governments,
18 the private sector, and other relevant stakeholders, shall
19 carry out a research, development, and demonstration pro-
20 gram to protect the electric grid and energy systems, in-
21 cluding assets connected to the distribution grid, from
22 cyber and physical attacks by increasing the cyber and
23 physical security capabilities of the energy sector and ac-
24 celerating the development of relevant technologies and
25 tools.

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

4

1 “(b) DEPARTMENT OF ENERGY.—As part of the ini-
2 tiative described in subsection (a), the Secretary shall
3 award research, development, and demonstration grants
4 to—

5 “(1) identify cybersecurity risks to information
6 systems within, and impacting, the electricity sector,
7 energy systems, and energy infrastructure;

8 “(2) develop methods and tools to rapidly detect
9 cyber intrusions and cyber incidents, including
10 through the use of data and big data analytics tech-
11 niques, such as intrusion detection, and security in-
12 formation and event management systems, to vali-
13 date and verify system behavior;

14 “(3) assess emerging cybersecurity capabilities
15 that could be applied to energy systems and develop
16 technologies that integrate cybersecurity features
17 and procedures into the design and development of
18 existing and emerging grid technologies, including
19 renewable energy, storage, and demand-side manage-
20 ment technologies;

21 “(4) identify existing vulnerabilities in intel-
22 ligent electronic devices, advanced analytics systems,
23 and information systems;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

5

1 “(5) work with relevant entities to develop tech-
2 nologies or concepts that build or retrofit cybersecu-
3 rity features and procedures into—

4 “(A) information and energy management
5 system devices, components, software, firmware,
6 and hardware, including distributed control and
7 management systems, and building manage-
8 ment systems;

9 “(B) data storage systems, data manage-
10 ment systems, and data analysis processes;

11 “(C) automated- and manually-controlled
12 devices and equipment for monitoring and sta-
13 bilizing the electric grid;

14 “(D) technologies used to synchronize time
15 and develop guidance for operational contin-
16 gency plans when time synchronization tech-
17 nologies, are compromised;

18 “(E) power system delivery and end user
19 systems and devices that connect to the grid,
20 including—

21 “(i) meters, synchrophasors, phasor
22 measurement units, and other sensors;

23 “(ii) distribution automation tech-
24 nologies, smart inverters, and other grid
25 control technologies;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

6

- 1 “(iii) distributed generation, energy
2 storage, and other distributed energy tech-
3 nologies;
4 “(iv) demand response technologies;
5 “(v) home and building energy man-
6 agement and control systems;
7 “(vi) electric and plug-in hybrid vehi-
8 cles and electric vehicle charging systems;
9 and
10 “(vii) other relevant devices, software,
11 firmware, and hardware; and
12 “(F) the supply chain of electric grid man-
13 agement system components;
14 “(6) develop technologies that improve the
15 physical security of information systems, including
16 remote assets;
17 “(7) integrate human factors research into the
18 design and development of advanced tools and proc-
19 esses for dynamic monitoring, detection, protection,
20 mitigation, response, and cyber situational aware-
21 ness;
22 “(8) evaluate and understand the potential con-
23 sequences of practices used to maintain the cyberse-
24 curity of information systems and intelligent elec-
25 tronic devices;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

7

1 “(9) develop or expand the capabilities of exist-
2 ing cybersecurity test beds to simulate impacts of
3 cyber attacks and combined cyber-physical attacks
4 on information systems and electronic devices, in-
5 cluding by increasing access to existing and emerg-
6 ing test beds for cooperative utilities, utilities owned
7 by a political subdivision of a State, such as munici-
8 pally-owned electric utilities, and other relevant
9 stakeholders; and

10 “(10) develop technologies that reduce the cost
11 of implementing effective cybersecurity technologies
12 and tools, including updates to these technologies
13 and tools, in the energy sector.

14 “(e) NATIONAL SCIENCE FOUNDATION.—The Na-
15 tional Science Foundation, in coordination with other Fed-
16 eral agencies as appropriate, shall through its cybersecu-
17 rity research and development programs—

18 “(1) support basic research to advance knowl-
19 edge, applications, technologies, and tools to
20 strengthen the cybersecurity of information systems,
21 including electric grid and energy systems, including
22 interdisciplinary research in—

23 “(A) evolutionary systems, theories, mathe-
24 matics, and models;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

8

1 “(B) economic and financial theories,
2 mathematics, and models; and

3 “(C) big data analytical methods, mathe-
4 matics, computer coding, and algorithms; and

5 “(2) support cybersecurity education and train-
6 ing focused on information systems for the electric
7 grid and energy workforce, including through the
8 Advanced Technological Education program, the
9 Cybercorps program, graduate research fellowships,
10 and other appropriate programs.

11 “(d) DEPARTMENT OF HOMELAND SECURITY
12 SCIENCE AND TECHNOLOGY DIRECTORATE.—The Science
13 and Technology Directorate of the Department of Home-
14 land Security shall coordinate with the Department of En-
15 ergy, the private sector, and other relevant stakeholders,
16 to research existing cybersecurity technologies and tools
17 used in the defense industry in order to—

18 “(1) identify technologies and tools that may
19 meet civilian energy sector cybersecurity needs;

20 “(2) develop a research strategy that incor-
21 porates human factors research findings to guide the
22 modification of defense industry cybersecurity tools
23 for use in the civilian sector;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

9

1 “(3) develop a strategy to accelerate efforts to
2 bring modified defense industry cybersecurity tools
3 to the civilian market; and

4 “(4) carry out other activities the Secretary of
5 Homeland Security considers appropriate to meet
6 the goals of this subsection.

7 **“SEC. 1311. GRID RESILIENCE AND EMERGENCY RESPONSE.**

8 “(a) IN GENERAL.—Not later than 180 days after
9 the enactment of the Grid Security Research and Develop-
10 ment Act, the Secretary shall establish a research, devel-
11 opment, and demonstration program to enhance resilience
12 and strengthen emergency response and management per-
13 taining to the energy sector.

14 “(b) GRANTS.—The Secretary shall award grants to
15 eligible entities under subsection (c) on a competitive basis
16 to conduct research and development with the purpose of
17 improving the resilience and reliability of electric grid by—

18 “(1) developing methods to improve community
19 and governmental preparation for and emergency re-
20 sponse to large-area, long-duration electricity inter-
21 ruptions, including through the use of energy effi-
22 ciency, storage, and distributed generation tech-
23 nologies;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

10

1 “(2) developing tools to help utilities and com-
2 munities ensure the continuous delivery of electricity
3 to critical facilities;

4 “(3) developing tools to improve coordination
5 between utilities and relevant Federal agencies to
6 enable communication, information-sharing, and sit-
7 uational awareness in the event of a physical or
8 cyber-attack on the electric grid;

9 “(4) developing technologies and capabilities to
10 withstand and address the current and projected im-
11 pact of the changing climate on energy sector infra-
12 structure, including extreme weather events and
13 other natural disasters;

14 “(5) developing technologies capable of early
15 detection of deteriorating electrical equipment on the
16 transmission and distribution grid, including detec-
17 tion of spark ignition causing wildfires and risks of
18 vegetation contact; and

19 “(6) assessing upgrades and additions needed
20 to energy sector infrastructure due to projected
21 changes in the energy generation mix and energy de-
22 mand.

23 “(c) ELIGIBLE ENTITIES.—The entities eligible to re-
24 ceive grants under this section include—

25 “(1) an institution of higher education;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

11

1 “(2) a nonprofit organization;
2 “(3) a National Laboratory;
3 “(4) a unit of State, local, or tribal government;
4 “(5) an electric utility or electric cooperative;
5 “(6) a retail service provider of electricity;
6 “(7) a private commercial entity;
7 “(8) a partnership or consortium of 2 or more
8 entities described in subparagraphs (1) through (7);
9 and

10 “(9) any other entities the Secretary deems ap-
11 propriate.

12 “(d) RELEVANT ACTIVITIES.—Grants awarded under
13 subsection (b) shall include funding for research and de-
14 velopment activities related to the purpose described in
15 subsection (b), such as—

16 “(1) development of technologies to use distrib-
17 uted energy resources, such as solar photovoltaics,
18 energy storage systems, electric vehicles, and
19 microgrids, to improve grid and critical end-user re-
20 silience;

21 “(2) analysis of non-technical barriers to great-
22 er integration and use of technologies on the dis-
23 tribution grid;

24 “(3) analysis of past large-area, long-duration
25 electricity interruptions to identify common elements

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

12

1 and best practices for electricity restoration, mitiga-
2 tion, and prevention of future disruptions;

3 “(4) development of advanced monitoring, ana-
4 lytics, operation, and controls of electricity grid sys-
5 tems to improve electric grid resilience;

6 “(5) analysis of technologies, methods, and con-
7 cepts that can improve community resilience and
8 survivability of frequent or long-duration power out-
9 ages;

10 “(6) development of methodologies to maintain
11 cybersecurity during restoration of energy sector in-
12 frastructure and operation;

13 “(7) development of advanced power flow con-
14 trol systems and components to improve electric grid
15 resilience; and

16 “(8) any other relevant activities determined by
17 the Secretary.

18 “(c) TECHNICAL ASSISTANCE.—

19 “(1) IN GENERAL.—The Secretary shall provide
20 technical assistance to eligible entities for the com-
21 mercial application of technologies to improve the re-
22 siliency of the electric grid and commercial applica-
23 tion of technologies to help entities develop plans for
24 preventing and recovering from various power out-
25 age scenarios at the local, regional, and State level.

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

13

1 “(2) TECHNICAL ASSISTANCE PROGRAM.—The
2 commercial application technical assistance program
3 established in paragraph (1) shall include assistance
4 to eligible entities for—

5 “(A) the commercial application of tech-
6 nologies developed from the grant program es-
7 tablished in subsection (b), including coopera-
8 tive utilities and utilities owned by a political
9 subdivision of a State, such as municipally-
10 owned electric utilities;

11 “(B) the development of methods to
12 strengthen or otherwise mitigate adverse im-
13 pacts on electric grid infrastructure against
14 natural hazards;

15 “(C) the use of Department data and mod-
16 eling tools for various purposes; and

17 “(D) a resource assessment and analysis of
18 future demand and distribution requirements,
19 including development of advanced grid archi-
20 tectures and risk analysis.

21 “(3) ELIGIBLE ENTITIES.—The entities eligible
22 to receive technical assistance for commercial appli-
23 cation of technologies under this section include—

24 “(A) representatives of all sectors of the
25 electric power industry, including electric utili-

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

14

1 ties, trade organizations, and transmission and
2 distribution system organizations, owners, and
3 operators;

4 “(B) State and local governments and reg-
5 ulatory authorities, including public utility com-
6 missions;

7 “(C) tribal and Alaska Native govern-
8 mental entities;

9 “(D) partnerships among entities under
10 subparagraphs (A) through (C);

11 “(E) regional partnerships; and

12 “(F) any other entities the Secretary
13 deems appropriate.

14 “(4) AUTHORITY.—Nothing in this section shall
15 authorize the Secretary to require any entity to
16 adopt any model, tool, technology, plan, analysis, or
17 assessment.

18 **“SEC. 1312. BEST PRACTICES AND GUIDANCE DOCUMENTS**
19 **FOR ENERGY SECTOR CYBERSECURITY RE-**
20 **SEARCH.**

21 “(a) IN GENERAL.—The Secretary, in coordination
22 with appropriate Federal agencies, the Electricity Sub-
23 sector Coordinating Council, standards development orga-
24 nizations, State, tribal, local, and territorial governments,
25 the private sector, public utility commissions, and other

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

15

1 relevant stakeholders, shall coordinate the development of
2 guidance documents for research, development, and dem-
3 onstration activities to improve the cybersecurity capabili-
4 ties of the energy sector through participating agencies.
5 As part of these activities, the Secretary shall—

6 “(1) facilitate stakeholder involvement to up-
7 date—

8 “(A) the Roadmap to Achieve Energy De-
9 livery Systems Cybersecurity;

10 “(B) the Cybersecurity Procurement Lan-
11 guage for Energy Delivery Systems, including
12 developing guidance for—

13 “(i) contracting with third parties to
14 conduct vulnerability testing for informa-
15 tion systems used across the energy pro-
16 duction, delivery, storage, and end use sys-
17 tems;

18 “(ii) contracting with third parties
19 that utilize transient devices to access in-
20 formation systems; and

21 “(iii) managing supply chain risks;
22 and

23 “(C) the Electricity Subsector Cybersecu-
24 rity Capability Maturity Model, including the

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

16

1 development of metrics to measure changes in
2 cybersecurity readiness; and

3 “(2) develop voluntary guidance to improve dig-
4 ital forensic analyses capabilities, including—

5 “(A) developing standardized terminology
6 and monitoring processes; and

7 “(B) utilizing human factors research to
8 develop more effective procedures for logging
9 incident events; and

10 “(3) work with the National Science Founda-
11 tion, Department of Homeland Security, and stake-
12 holders to develop a mechanism to anonymize, ag-
13 gregate, and share the testing results from cyberse-
14 curity test beds to facilitate technology improve-
15 ments by public and private sector researchers.

16 “(c) BEST PRACTICES.—The Secretary, in collabora-
17 tion with the Director of the National Institute of Stand-
18 ards and Technology and other appropriate Federal agen-
19 cies, shall convene relevant stakeholders and facilitate the
20 development of—

21 “(1) consensus-based best practices to improve
22 cybersecurity for—

23 “(A) emerging energy technologies;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

17

1 “(B) distributed generation and storage
2 technologies, and other distributed energy re-
3 sources;

4 “(C) electric vehicles and electric vehicle
5 charging stations; and

6 “(D) other technologies and devices that
7 connect to the electric grid;

8 “(2) recommended cybersecurity features and
9 requirements that can be used by the private sector
10 to design and build interoperable cybersecurity fea-
11 tures into technologies that connect to the electric
12 grid, including networked devices and components
13 on distribution systems; and

14 “(3) technical analysis that can be used by the
15 private sector in developing best practices for test
16 beds and test bed methodologies that will enable re-
17 producible testing of cybersecurity protections for in-
18 formation systems, electronic devices, and other rel-
19 evant components, software, and hardware across
20 test beds.

21 “(d) REGULATORY AUTHORITY.—None of the activi-
22 ties authorized in this section shall be construed to author-
23 ize regulatory actions. Additionally, the voluntary stand-
24 ards developed under this section shall not duplicate or
25 conflict with mandatory reliability standards.

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

18

1 **"SEC. 1313. VULNERABILITY TESTING AND TECHNICAL AS-**
2 **SISTANCE TO IMPROVE CYBERSECURITY.**

3 "(a) IN GENERAL.—The Secretary shall—

4 "(1) coordinate with energy sector asset owners
5 and operators, leveraging the research facilities and
6 expertise of the National Laboratories, to assist enti-
7 ties in developing testing capabilities by—

8 "(A) utilizing a range of methods to iden-
9 tify vulnerabilities in physical and cyber sys-
10 tems;

11 "(B) developing cybersecurity risk assess-
12 ment tools and providing analyses and rec-
13 ommendations to participating stakeholders;
14 and

15 "(C) working with stakeholders to develop
16 methods to share anonymized and aggregated
17 test results to assist relevant stakeholders in
18 the energy sector, researchers, and the private
19 sector to advance cybersecurity efforts, tech-
20 nologies, and tools;

21 "(2) collaborate with relevant stakeholders, in-
22 cluding public utility commissions, to—

23 "(A) identify information, research, staff
24 training, and analytical tools needed to evaluate
25 cybersecurity issues and challenges in the en-
26 ergy sector; and

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

1 “(B) facilitate the sharing of information
2 and the development of tools identified under
3 subparagraph (A);

4 “(3) collaborate with tribal governments to
5 identify information, research, and analysis tools
6 needed by tribal governments to increase the cyber-
7 security of energy assets within their jurisdiction.

8 **“SEC. 1314. EDUCATION AND WORKFORCE TRAINING RE-**
9 **SEARCH AND STANDARDS.**

10 “(a) IN GENERAL.—The Secretary shall support the
11 development of a cybersecurity workforce through a pro-
12 gram that—

13 “(1) facilitates collaboration between under-
14 graduate and graduate students, researchers at the
15 National Laboratories, and the private sector;

16 “(2) prioritizes science and technology in areas
17 relevant to the mission of the Department of Energy
18 through the design and application of cybersecurity
19 technologies;

20 “(3) develops, or facilitates private sector devel-
21 opment of, voluntary cybersecurity training and re-
22 training standards, lessons, and recommendations
23 for the energy sector that minimize duplication of
24 cybersecurity compliance training programs; and

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

20

1 “(4) maintains a public database of cybersecu-
2 rity education, training, and certification programs.

3 “(b) COLLABORATION.—In carrying out the program
4 authorized in subsection (a), the Secretary shall leverage
5 programs and activities carried out across the Department
6 of Energy, other relevant Federal agencies, institutions of
7 higher education, and other appropriate entities best suit-
8 ed to provide national leadership on cybersecurity-related
9 issues.

10 **“SEC. 1315. INTERAGENCY COORDINATION AND STRATEGIC**
11 **PLAN FOR ENERGY SECTOR CYBERSECURITY**
12 **RESEARCH.**

13 “(a) DUTIES.—The Secretary, in coordination with
14 the Energy Sector Government Coordinating Council,
15 shall—

16 “(1) review the most recent versions of the
17 Roadmap to Achieve Energy Delivery Systems Cy-
18 bersecurity and the Multi-Year Program Plan for
19 Energy Sector Cybersecurity to identify crosscutting
20 energy sector cybersecurity research needs and op-
21 portunities for collaboration among Federal agencies
22 and other relevant stakeholders;

23 “(2) identify interdisciplinary research, tech-
24 nology, and tools that can be applied to cybersecu-
25 rity challenges in the energy sector;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

21

1 “(3) identify technology transfer opportunities
2 to accelerate the development and commercial appli-
3 cation of novel cybersecurity technologies, systems,
4 and processes in the energy sector; and

5 “(4) develop a coordinated Interagency Stra-
6 tegic Plan for research to advance cybersecurity ca-
7 pabilities used in the energy sector that builds on
8 the Roadmap to Achieve Energy Delivery Systems in
9 Cybersecurity and the Multi-Year Program Plan for
10 Energy Sector Cybersecurity.

11 “(b) INTERAGENCY STRATEGIC PLAN.—

12 “(1) SUBMITTAL.—The Interagency Strategic
13 Plan developed under subsection (a)(4) shall be sub-
14 mitted to Congress within 12 months after the date
15 of enactment of the Grid Security Research and De-
16 velopment Act.

17 “(2) CONTENTS.—The Interagency Strategic
18 Plan shall include—

19 “(A) an analysis of how existing cybersecu-
20 rity research efforts across the Federal Govern-
21 ment are advancing the goals of the Roadmap
22 to Achieve Energy Delivery Systems Cybersecu-
23 rity and the Multi-Year Program Plan for En-
24 ergy Sector Cybersecurity;

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

22

1 “(B) recommendations for research areas
2 that may advance the cybersecurity of the en-
3 ergy sector;

4 “(C) an overview of existing and proposed
5 public and private sector research efforts that
6 address the topics outlined in paragraph (3);
7 and

8 “(D) an overview of needed support for
9 workforce training in cybersecurity for the en-
10 ergy sector.

11 “(3) CONSIDERATIONS.—In developing the
12 Interagency Strategic Plan, the Secretary, in coordi-
13 nation with the Energy Sector Government Coordi-
14 nating Council, shall consider—

15 “(A) opportunities for human factors re-
16 search to improve the design and effectiveness
17 of cybersecurity devices, technologies, tools,
18 processes, and training programs;

19 “(B) contributions of other disciplines to
20 the development of innovative cybersecurity pro-
21 cedures, devices, components, technologies, and
22 tools;

23 “(C) opportunities for technology transfer
24 programs to facilitate private sector develop-
25 ment of cybersecurity procedures, devices, com-

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

23

1 ponents, technologies, and tools for the energy
2 sector;

3 “(D) broader applications of the work done
4 by relevant Federal agencies to advance the cy-
5 bersecurity of information systems and data
6 analytics systems for the energy sector; and

7 “(E) activities called for in the Federal cy-
8 bersecurity research and development strategic
9 plan required by section 201(a)(1) of the Cy-
10 bersecurity Enhancement Act of 2014 (15
11 U.S.C. 7431(a)(1)).

12 “(e) PARTICIPATION.—For the purposes of carrying
13 out this section, the Energy Sector Government Coordi-
14 nating Council shall include representatives from Federal
15 agencies with expertise in the energy sector, information
16 systems, data analytics, cyber physical systems, engineer-
17 ing, human factors research, human-machine interfaces,
18 high performance computing, big data and data analytics,
19 or other disciplines considered appropriate by the Council
20 Chair.

21 **“SEC. 1316. REPORT TO CONGRESS.**

22 **“(a) BALANCING RISKS, INCREASING SECURITY, AND**
23 **IMPROVING MODERNIZATION.—**

24 “(1) STUDY.—The Secretary, in collaboration
25 with the National Institute of Standards and Tech-

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

24

1 nology, other Federal agencies, and energy sector
2 stakeholders, in order to provide recommendations
3 for additional research, development, demonstration,
4 and commercial application activities, shall—

5 “(A) analyze physical and cyber attacks on
6 energy sector infrastructure and information
7 systems and identify cost-effective opportunities
8 to improve physical and cyber security; and

9 “(B) examine the risks associated with in-
10 creasing penetration of digital technologies in
11 grid networks, particularly on the distribution
12 grid.

13 “(2) CONTENT.—The study shall—

14 “(A) analyze processes, operational proce-
15 dures, and other factors common among cyber
16 attacks;

17 “(B) identify areas where human behavior
18 plays a critical role in maintaining or compro-
19 mising the security of a system;

20 “(C) recommend—

21 “(i) changes to the design of devices,
22 human-machine interfaces, technologies,
23 tools, processes, or procedures to optimize
24 security that do not require a change in
25 human behavior; and

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

25

1 “(ii) training techniques to increase
2 the capacity of employees to actively iden-
3 tify, prevent, or neutralize the impact of
4 cyber attacks;

5 “(D) evaluate existing engineering and
6 technical design criteria and guidelines that in-
7 corporate human factors research findings, and
8 recommend criteria and guidelines for cyberse-
9 curity tools that can be used to develop display
10 systems for cybersecurity monitoring, such as
11 alarms, user-friendly displays, and layouts;

12 “(E) evaluate the cybersecurity risks and
13 benefits of various design and architecture op-
14 tions for energy sector systems, networked grid
15 systems and components, and automation sys-
16 tems, including consideration of—

17 “(i) designs that include both digital
18 and analog control devices and tech-
19 nologies;

20 “(ii) different communication tech-
21 nologies used to transfer information and
22 data between control system devices, tech-
23 nologies, and system operators;

24 “(iii) automated and human-in-the-
25 loop devices and technologies;

G:\CMTE\SC\16\ENERGY\GRIDCYBERSECURITYACT_2.XML

26

1 “(iv) programmable versus non-
2 programmable devices and technologies;

3 “(v) increased redundancy using dis-
4 similar cybersecurity technologies; and

5 “(vi) grid architectures that use au-
6 tonomous functions to limit control
7 vulnerabilities; and

8 “(F) recommend methods or metrics to
9 document changes in risks associated with sys-
10 tem designs and architectures.

11 “(3) CONSULTATION.—In conducting the study,
12 the Secretary shall consult with energy sector stake-
13 holders, academic and private sector researchers, the
14 private sector, and other relevant stakeholders.

15 “(4) REPORT.—Not later than 24 months after
16 the date of enactment of the Grid Security Research
17 and Development Act, the Secretary shall submit the
18 study to the Committee on Science, Space, and
19 Technology of the House of Representatives and the
20 Committee on Energy and Natural Resources of the
21 Senate.

22 **“SEC. 1317. DEFINITIONS.**

23 **“In this title:**

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

27

1 “(1) BIG DATA.—The term ‘big data’ means
2 datasets that require advanced analytical methods
3 for their transformation into useful information.

4 “(2) CYBERSECURITY.—The term ‘cybersecu-
5 rity’ means protecting an information system or in-
6 formation that is stored on, processed by, or
7 transiting an information system from a cybersecu-
8 rity threat or security vulnerability.

9 “(3) CYBERSECURITY THREAT.—The term ‘cy-
10 bersecurity threat’ has the meaning given the term
11 in section 102 of the Cybersecurity Information
12 Sharing Act of 2015 (6 U.S.C. 1501).

13 “(4) ELECTRICITY SUBSECTOR COORDINATING
14 COUNCIL.—The term ‘Electricity Subsector Coordi-
15 nating Council’ means the self-organized, self-gov-
16 erned council consisting of senior industry represent-
17 atives to serve as the principal liaison between the
18 Federal Government and the electric power sector
19 and to carry out the role of the Sector Coordinating
20 Council as established in the National Infrastructure
21 Protection Plan for the electricity subsector.

22 “(5) ENERGY SECTOR GOVERNMENT COORDI-
23 NATING COUNCIL.—The term ‘Energy Sector Gov-
24 ernment Coordinating Council’ means the council
25 consisting of representatives from relevant Federal

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

28

1 Government agencies to provide effective coordina-
2 tion of energy sector efforts to ensure a secure, reli-
3 able, and resilient energy infrastructure and to carry
4 out the role of the Government Coordinating Council
5 as established in the National Infrastructure Protec-
6 tion Plan for the energy sector.

7 “(6) HUMAN FACTORS RESEARCH.—The term
8 ‘human factors research’ means research on human
9 performance in social and physical environments,
10 and on the integration and interaction of humans
11 with physical systems and computer hardware and
12 software.

13 “(7) HUMAN-MACHINE INTERFACES.—The term
14 ‘human-machine interfaces’ means technologies that
15 present information to an operator or user about the
16 state of a process or system, or accept human in-
17 structions to implement an action, including visual-
18 ization displays such as a graphical user interface.

19 “(8) INFORMATION SYSTEM.—The term ‘infor-
20 mation system’—

21 “(A) has the meaning given the term in
22 section 102 of the Cybersecurity Information
23 Sharing Act of 2015 (6 U.S.C. 1501); and

24 “(B) includes operational technology, infor-
25 mation technology, and communications.

G:\CMTE\SC\16\ENERGY\GRID\CYBERSECURITY\ACT_2.XML

1 “(9) NATIONAL LABORATORY.—The term ‘na-
2 tional laboratory’ has the meaning given the term in
3 section 2 of the Energy Policy Act of 2005 (42
4 U.S.C. 15801).

5 “(10) SECURITY VULNERABILITY.—The term
6 ‘security vulnerability’ has the meaning given the
7 term in section 102 of the Cybersecurity Information
8 Sharing Act of 2015 (6 U.S.C. 1501).

9 “(11) TRANSIENT DEVICES.—The term ‘tran-
10 sient devices’ means removable media, including
11 floppy disks, compact disks, USB flash drives, exter-
12 nal hard drives, mobile devices, and other devices
13 that utilize wireless connections.

14 **“SEC. 1318. AUTHORIZATION OF APPROPRIATIONS.**

15 “There are authorized to be appropriated to the Sec-
16 retary to carry out this title—

17 “(1) \$150,000,000 for fiscal year 2021;

18 “(2) \$157,500,000 for fiscal year 2022;

19 “(3) \$165,375,000 for fiscal year 2023;

20 “(4) \$173,645,000 for fiscal year 2024; and

21 “(5) \$182,325,000 for fiscal year 2025.”.

Chairwoman JOHNSON. Without objection, the bill is considered as read and open to amendment at any point. I recognize the gentleman from California, Mr. Bera, to speak on his bill.

Mr. BERA. Thank you, Chairwoman Johnson, Ranking Member Lucas. I'm proud that—today that our Committee is advancing bipartisan legislation to address threats to our electrical grid. A strong and secure electrical grid is critical to our quality of life, economy, and national security. However, the cybersecurity landscape is constantly evolving with attacks on the grid becoming more and more frequent.

Last year, remote hackers attacked the U.S. grid networks for the first time affecting several Western States, including California, Utah, and Wyoming. Following this attack, the President and CEO of the North American Electric Reliability Corporation, NERC, testified before Congress in July stating the threat from cybersecurity attack is at an all-time high.

In addition, our electric grid is increasingly more vulnerable to natural disasters like wildfires and hurricanes. From coast to coast the United States has been hit by major hurricanes, storms, and wildfires that have left Americans without electricity, disrupting daily life and crippling local economies. Hearing from my constituents regarding the California wildfires made it abundantly clear that protecting the electrical grid was a priority for them.

That's why I'm proud to introduce the bipartisan *Grid Security Research and Development Act* alongside Congressman Weber to strengthen the resiliency of the U.S. electric grid and protect the American public. Our legislation focuses on sustained investment in research and technologies to keep pace with the rapidly evolving threats to our electric grid. The bill focuses on protecting our grid from two major threats: cyber and physical.

I'm also proud that this bill would provide funding to develop technologies that would toughen our grid against wildfires and other natural disasters by improving early detection of deteriorating electrical transmission and distribution equipment that can tend to spark and come in contact with vegetation during high wind events and natural disasters that cause wildfires.

My bill, in tandem with the four other important energy bills that are being considered today, take a holistic approach to driving toward a cleaner and safer future for the American public. We're here to make government work for our constituents and for the American people and to address their concerns and create solutions.

Thank you again, Chairwoman Johnson, Ranking Member Lucas, for supporting this important priority for California and for America, and I urge my colleagues to support this legislation. I yield back.

Chairwoman JOHNSON. Thank you very much. Anyone else seeking time?

Mr. WEBER. Madam Chair, I move to strike the last word.

Chairwoman JOHNSON. Mr. Weber.

Mr. WEBER. Thank you, Madam Chair. And thank you, Madam Chair and Ranking Member Lucas, for holding today's markup.

I am also, like my colleague from California, proud to speak this morning in support of H.R. 5760, the *Grid Security Research and Development Act*, of which I am an original cosponsor.

Folks, a secure, resilient, and reliable electric grid is essential to America's national and economic security. When I speak to crowds, I will often say the things that make America great are the things that America makes. How do we do that? Again, with a secure, resilient, and reliable electrical grid. It is absolutely essential.

Every aspect of our daily lives and every economic sector in our Nation depends on the uninterrupted flow of power to function properly. Recognizing this, the Trump Administration has consistently emphasized the importance of grid cybersecurity, of resilience, and emergency response, and has made these issues a major priority.

Cyber and physical threats to our electric grid are constantly evolving and increasing in magnitude. According to IBM, last year, cyber attacks against vital energy sector technologies like industrial control and operational systems increased by more than 2,000 percent from 2018. In fact, in 2019 in the United States our energy sector ranked ninth in the industries most targeted by cyber attacks. So it is clear that this bipartisan legislation is both timely and absolutely necessary.

H.R. 5760, the *Grid Security Research and Development Act*, authorizes a multiagency research and development program to bolster the cyber and physical security capabilities of this very energy sector. It also authorizes key Federal agencies like DOE and the National Science Foundation to support early stage research, development, and demonstration activities that will advance critical energy sector cybersecurity technologies while improving the security of energy sector information systems. It is in line with this Administration's priorities, H.R. 5760. It also authorizes a DOE research, development, and demonstration program that focuses on the discovery of new innovative tools and new technologies that will improve the resilience, reliability, and emergency response capabilities of our electric grid.

Just three years ago Hurricane Harvey hit the Texas Gulf Coast, my district, ground zero for Harvey flooding. Hurricane Harvey caused significant damage to generators and transmission lines and outages for many homes and businesses in my very district. Luckily, the Electric Reliability Council of Texas, ERCOT as we call it, was up to date on their planning and management. The Texas grid was able to quickly recover from a devastating category 4 hurricane. That's just one example of how it is not a question of if the U.S. power grid will face a significant physical or cyber threat, it is simply a matter of when.

The modernization and security of the national electricity system must be one of our top priorities. I want to thank Dr. Bera for introducing this legislation and Members and staff on both sides of the aisle for working in such a collaborative manner to prepare this bill for today's markup. I encourage my colleagues to support this timely bipartisan legislation to improve the cyber and physical security of our Nation's very energy sector.

Madam Chair, I appreciate you, and I yield back the balance of my time.

Chairwoman JOHNSON. Thank you very much. Any other requests for time?

We will now proceed with amendments in the order on the roster. And the first amendment on the roster is the amendment offered by Mr. Bera, and he's recognized to offer an amendment.

Mr. BERA. I have an amendment at the desk.

Chairwoman JOHNSON. The clerk will report the amendment.

The CLERK. Amendment No. 1, amendment to H.R. 5760—

[The amendment of Mr. Bera follows:]

71

182

G:\CMTE\SC\16\ENERGY\H5760\MNGR-AMDT_01.XML

AMENDMENT TO H.R. 5760

OFFERED BY Mr . Bera

Page 2, line 14, strike “(5)” and insert “(4)”.

Page 2, line 19, strike “(6)” and insert “(5)”.

Page 2, line 25, strike “(7)” and insert “(6)”.

Page 5, line 21, strike “synchrophasors,”.

Page 10, line 15, strike “deteriorating” and insert
“malfunctioning”.

Page 10, line 18, strike “and”.

Page 10, line 22, strike the period and insert “;
and”.

Page 10, after line 22, insert the following:

1 “(7) upgrading tools used to estimate the costs
2 of outages longer than 24 hours.

Page 12, line 4, strike “electricity” and insert “elec-
tric”.

Page 16, line 4, strike “analyses” and insert “anal-
ysis”.

Page 16, line 16, strike “(c)” and insert “(b)”.

72

183

G:\CMTE\SC\16\ENERGY\H5760\MNGR-AMDT_01.XML

2

Page 17, line 8, strike “features and” and insert
“designs and technical”.

Page 17, line 21, strike “(d)” and insert “(e)”.

Page 21, line 14, strike “Congress” and insert
“Congress and made public”.

Page 23, line 16, strike “cyber” and insert “cyber
and”.

Page 26, line 13, strike “and private sector”.

Page 29, line 16, strike “title” and insert “Act”.



Chairwoman JOHNSON. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

I recognize the gentleman for five minutes to explain his amendment.

Mr. BERA. Thank you, Chairwoman Johnson and Ranking Member Lucas. I rise to offer a manager's amendment to offer technical corrections to the bill like wording and line numbering.

As I emphasized before, the bill will support important research and development to address the evolving cybersecurity threats to our grid and ensure that our grid is resilient to disasters like hurricanes, floods, and the terrible wildfires which have spread across my home State of California. I encourage all of my colleagues to support my amendment, and with that, I yield back.

Chairwoman JOHNSON. Thank you. Any further discussion on the amendment?

If there's no further discussion, the vote occurs on the amendment.

All those in favor, say aye.

Those opposed, say no.

The ayes have it, and the amendment is agreed to.

The next amendment on the roster is an amendment offered by the gentlelady from California, Ms. Lofgren, and Mr. McNerney is recognized.

Mr. MCNERNEY. Madam Chair, I have an amendment at the desk.

Chairwoman JOHNSON. The clerk will report the amendment.

The CLERK. Amendment No. 2, amendment to H.R.—

[The amendment of Ms. Lofgren follows:]

74

185

G:\M\16\LOFGRE\LOFGRE_027.XML

AMENDMENT TO H.R. 5760
OFFERED BY MS. LOFGREN OF CALIFORNIA

Page 10, line 18, strike “and”.

Page 10, line 22, strike the period and insert “;
and”.

Page 10, after line 22, insert the following:

1 “(7) developing tools and technologies to assist
2 with the planning, safe execution of, and safe and
3 timely restoration of power after emergency power
4 shut offs, such as those conducted to reduce risks of
5 wildfires started by grid infrastructure.

Page 13, line 16, strike “and”.

Page 13, line 20, strike the period at the end and
insert a semicolon.

Page 13, after line 20, insert the following:

6 “(E) the development of tools and tech-
7 nologies to coordinate data across relevant enti-
8 ties to promote resilience and wildfire preven-
9 tion in the planning, design, construction, oper-
10 ation, and maintenance of transmission infra-
11 structure;

G:\M\16\LOFGRE\LOFGRE_027.XML

2

1 “(F) analysis to predict the likelihood of
2 extreme weather events to inform the planning,
3 design, construction, operation, and mainte-
4 nance of transmission infrastructure in con-
5 sultation with the National Oceanic and Atmos-
6 pheric Administration; and
7 “(G) the commercial application of rel-
8 evant technologies, such as distributed energy
9 resources, microgrids, or other energy tech-
10 nologies, to establish backup power for users or
11 facilities affected by emergency power shutoffs.

Page 20, after line 2, insert the following:

12 “(b) GRID RESILIENCE TECHNOLOGY TRAINING.—
13 The Secretary shall support the development of the grid
14 workforce through a training program that prioritizes ac-
15 tivities that enhance the resilience of the electric grid and
16 energy sector infrastructure, including training on the use
17 of tools, technologies, and methods developed under the
18 grant program established in section 1311(b).

Page 20, line 3, strike “(b)” and insert “(c)”.

Page 20, line 4, insert “and (b)” after “authorized
in subsection (a)”.

76

187

G:\M\16\LOFGRE\LOFGRE_027.XML

3

Page 20, line 8, insert “and grid resilience” after
“cybersecurity”.



Chairwoman JOHNSON. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

I recognize the gentleman to explain the amendment for five minutes.

Mr. MCNERNEY. Thank you, Madam Chair.

The needs and challenges surrounding our grid infrastructure have changed considerably since Congress passed the last significant legislation in this area. Traditionally, the conversation around grid resilience has been how to harden the grid without natural disasters—to withstand natural disasters. However, we now have the problem of electric grid infrastructure starting wildfires, especially in my State of California. States prone to wildfires have been working on this issue for a while, and it's time for the Federal Government to catch up. This amendment would help address that. Significant investments at the Federal level on research and technology are necessary to ensure the safety, continuous delivery, and reliability of electricity across all States.

So I want to thank my colleagues Mr. Lamb and Mr. Bera for introducing H.R. 5428 and H.R. 5760 on R&D for grid modernization and security.

Last year in Northern California, we had several large, long-duration power outages, including ones that affected my home, better known as public safety power shutoff events, meant to prevent wildfires sparked by electric grid infrastructure during extreme wind and dry conditions.

My amendment, or Ms. Lofgren's amendment, would provide for the improvement in execution of emergency power shutoffs from the planning to the power restoration through a grant program established in section 1311. While there's a considerable amount of data being collected in this space, States need the tools to standardize and coordinate this data across all relevant entities for the purposes of not just emergency response but for the planning, design, construction, operation, and maintenance of transmission infrastructure. My amendment—again, Ms. Lofgren's amendment, would provide technical assistance to relevant entities looking to do just that.

Lastly, we have a workforce shortage in the area due to sudden growth in demand for individuals qualified and trained in grid resilience technology. This amendment would establish a training program to support the development of the grid workforce through the use of tools, technologies, and methods developed under the grant program. I urge my colleagues to support this amendment, and I yield back the balance of my time.

Chairwoman JOHNSON. Thank you very much. Any further discussion on the amendment?

If there's no further discussion, the vote occurs on the amendment.

All in favor, say aye.

Those opposed, no.

The ayes have it, and the amendment is agreed to.

The next amendment on the roster is an amendment offered by the gentleman from Florida, Mr. Waltz, and he's recognized for five minutes to offer his amendment.

Mr. WALTZ. Thank you, Madam Chairwoman. I have an amendment at the desk.

Chairwoman JOHNSON. The clerk will report the amendment.

The CLERK. Amendment No. 3, amendment to Committee print—

[The amendment of Mr. Waltz follows:]

G:\CMTE\SC\16\ENERGY\H5760\RAMD1.XML

AMENDMENT TO
COMMITTEE PRINT OF H.R. 5760
OFFERED BY M. _____

Add at the end the following:

1 SEC. 4. CRITICAL INFRASTRUCTURE RESEARCH AND CON-
2 STRUCTION.

3 (a) IN GENERAL.—The Secretary shall carry out a
4 program of research, development, and demonstration of
5 technologies and tools to help ensure the resilience and
6 security of critical integrated grid infrastructures.

7 (b) CRITICAL INFRASTRUCTURE DEFINED.—The
8 term “critical infrastructure” means infrastructure that
9 the Secretary determines to be vital to socioeconomic ac-
10 tivities such that, if destroyed or damaged, such destruc-
11 tion or damage could cause substantial disruption to such
12 socioeconomic activities.

13 (c) COORDINATION.—In carrying out the program
14 under subsection (a), the Secretary shall leverage expertise
15 and resources of and facilitate collaboration and coordina-
16 tion between—

- 17 (1)** relevant programs and activities across the
- 18** Department;
- 19 (2)** the Department of Defense; and

G:\CMTE\SC\16\ENERGY\H5760\RAMD1.XML

2

1 (3) the Department of Homeland Security.

2 (d) CRITICAL INFRASTRUCTURE TEST FACILITY.—In
3 carrying out the program under subsection (a), the Sec-
4 retary shall establish and operate a Critical Infrastructure
5 Test Facility (referred to in this section as the “Test Fa-
6 cility”) that allows for scalable physical and cyber per-
7 formance testing to be conducted on industry-scale critical
8 infrastructure systems. This facility shall include a focus
9 on—

10 (1) cybersecurity test beds; and

11 (2) electric grid test beds.

12 (e) SELECTION.—The Secretary shall select the Test
13 Facility under this section on a competitive, merit-re-
14 viewed basis. The Secretary shall consider applications
15 from National Laboratories, institutions of higher edu-
16 cation, multi-institutional collaborations, and other appro-
17 priate entities.

18 (f) DURATION.—The Test Facility established under
19 this section shall receive support for a period of not more
20 than 5 years, subject to the availability of appropriations.

21 (g) RENEWAL.—Upon the expiration of any period of
22 support of the Test Facility, the Secretary may renew sup-
23 port for the Test Facility, on a merit-reviewed basis, for
24 a period of not more than 5 years.

81

192

G:\CMTE\SC\16\ENERGY\H5760\RAMD1.XML

3

1 (h) TERMINATION.—Consistent with the existing au-
2 thorities of the Department, the Secretary may terminate
3 the Test Facility for cause during the performance period.



Chairwoman JOHNSON. I ask unanimous consent to dispense with the reading. Without objection, so ordered.

And I recognize the gentleman for five minutes to explain his amendment.

Mr. WALTZ. Thank you, Madam Chairwoman, Ranking Member Lucas.

This amendment to H.R. 5760, the *Grid Security Research and Development Act*, requires the Secretary of Energy to carry out a program in coordination with the Department of Defense and the Department of Homeland Security to help ensure the security and resilience of critical grid infrastructures. In carrying out this program, it also requires the Secretary to establish and operate a critical infrastructure test facility that allows for both physical and cyber performance testing to be conducted on large-scale infrastructure systems.

The goal of this research is to improve the development of new energy technologies, advance our understandings of integrated grid systems. A dedicated critical infrastructure test facility can provide American researchers with access to cybersecurity and electric grid testbeds that are necessary to perform this next-generation R&D. As more industrial control systems come online, and as a diversity of energy sources are integrated into the grid, we must invest strategically in the long-term early stage research that will protect our energy infrastructure from a variety of emerging threats.

The investments authorized in my amendment will do just that, and they will act as an accelerator to the R&D programs authorized in H.R. 5760, driving forward innovation and maximizing return on taxpayer dollars. The partnership between the Federal Government, the national labs, academia, and industry has the potential to transform energy delivery systems.

I look forward to working with my colleagues on both sides of the aisle as we continue supporting advanced grid security research and our shared mission goals to develop future energy delivery systems that are reliable, resilient, and secure. I encourage my colleagues to support this amendment and yield back the balance of my time.

Chairwoman JOHNSON. Thank you. Any further discussion on the amendment?

If there's no further discussion, the vote occurs on the amendment.

All those in favor, say aye.

Those opposed, no.

The ayes have it, and the agreement—and the amendment is agreed to.

Are there any other amendments?

A reporting quorum being present, I move that the Committee on Science, Space, and Technology report H.R. 5760, as amended, to the House with the recommendation that the bill be approved.

Those in favor of the motion will signify by saying aye.

Those opposed, no.

The ayes have it, and the bill is favorably reported.

Without objection, the motion to reconsider is laid upon the table. I ask unanimous consent that the staff be authorized to make any

necessary technical and conforming changes to the bill. Without objection, so ordered.

Members will have two subsequent calendar days in which to submit supplementary minority or additional views on this measure.

I want to thank all of the Members in attendance. And that concludes our markup. The Committee is adjourned.

[Whereupon, at 11:27 a.m., the Committee was adjourned.]

